IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

LOUJAIN HATHLOUL ALHATHLOUL, Plaintiff, v. **DARKMATTER GROUP**; **MARK BAIER**; **RYAN ADAMS**; and **DANIEL GERICKE**, Defendants.	Case No. 3:21-cv-01787-IM **OPINION AND ORDER GRANTING IN PART AND DENYING IN PART DEFENDANTS' MOTIONS TO DISMISS**

Stephanie J. Grant, Tonkon Torp LLP, 888 SW Fifth Avenue, Suite 1600, Portland, OR 97204; Christopher E. Hart, Anthony D. Mirenda, Andrew Loewenstein & Allen M. Thigpen, Foley Hoag LLP, 155 Seaport Boulevard, Boston, MA 02210; Daniel McLaughlin, Claret Vargas & Carmen Cheung Ka-Man, Center for Justice and Accountability, 268 Bush Street #3432, San Francisco, CA 94104; and David Greene & Sophia Cope, Electronic Frontier Foundation, 815 Eddy Street, San Francisco, CA 94109. Attorneys for Plaintiff Loujain Hathloul Alhathloul.

Nika Aldrich, Schwabe, Williamson & Wyatt, P.C., 1211 SW Fifth Avenue, Suite 1900, Portland, OR 97204; and Anthony T. Pierce, James E. Tysse & Caroline L. Wolverton, Akin Gump Strauss Hauer & Feld LLP, 2001 K Street NW, Washington, DC 20006. Attorneys for Defendant DarkMatter Group.

Clifford S. Davidson, Snell & Wilmer LLP, 601 SW Second Avenue, Suite 2000, Portland, OR 97204. Attorney for Defendants Marc Baier, Ryan Adams, and Daniel Gericke.

IMMERGUT, District Judge.

This case involves allegedly unlawful actions by Defendant DarkMatter Group ("DarkMatter"), a software company based in the United Arab Emirates, and three of its former senior executives, Marc Baier, Ryan Adams, and Daniel Gericke (the "individual Defendants" and, together with DarkMatter, the "Defendants"). Plaintiff Loujain Alhathloul, a prominent Saudi women's rights activist, alleges the Defendants hacked her iPhone, surveilled her movements, and exfiltrated her private data. First Amended Complaint ("FAC"), ECF 54. Plaintiff alleges the hack facilitated her arrest in the United Arab Emirates and rendition to Saudi Arabia, where she alleges she was imprisoned and tortured. *Id.* Plaintiff alleges all Defendants violated the Computer Fraud and Abuse Act ("CFAA"), *id.* ¶¶ 178–214, and conspired together and with Emirati officials to violate the CFAA, *id.* ¶¶ 215–26. She also alleges the individual Defendants' actions constitute a crime against humanity actionable under the Alien Tort Statute ("ATS"). *Id.* ¶¶ 227–34.

Now before this Court are two motions to dismiss Plaintiff's FAC. First, all Defendants move to dismiss the FAC for lack of personal jurisdiction and for failure to state a claim under the CFAA. Defendants' Joint Second Motion to Dismiss First Amended Complaint ("MTD"), ECF 126. Second, the individual Defendants move to dismiss Plaintiff's ATS claim, arguing this Court lacks subject-matter jurisdiction over that claim. Individual Defendants' Joint Motion to Dismiss the Alien Tort Statute Claim for Lack of Subject-Matter Jurisdiction ("ATS MTD"), ECF 127.

This Court concludes Plaintiff's FAC makes a prima facie showing of specific personal jurisdiction over all Defendants. Plaintiff's allegations that Defendants committed an intentional tort while Plaintiff was in the U.S., together with Defendants' other forum-related contacts,

establish minimum contacts that arise out of Plaintiff's claims, and Defendants have failed to establish that exercising jurisdiction would be unreasonable. The motion to dismiss for lack of personal jurisdiction is therefore denied. This Court also denies Defendants' motion to dismiss Plaintiff's CFAA and CFAA conspiracy claims. Finally, this Court declines to recognize Plaintiff's alleged tort of discriminatory persecution under the ATS and accordingly grants the individual Defendants' motion to dismiss that claim for lack of subject-matter jurisdiction.

BACKGROUND

For purposes of the motions to dismiss, this Court takes the allegations of the complaint, summarized here, as true.

A. The Parties and Project Raven

Plaintiff Loujain Hathloul Alhathloul is a prominent Saudi human rights activist, notable for her advocacy against Saudi Arabia's ban on women driving and its male guardianship system. FAC, ECF 54 ¶¶ 16–29. Among other efforts, in 2016, she organized a petition directly to Saudi's King Salman calling for the end of male guardianship. *Id.* ¶ 22. Plaintiff has built her campaign using her own name rather than a pseudonym. *Id.* ¶ 18. Plaintiff's public advocacy has garnered international support from activists in the U.S., *id.* ¶¶ 23–26, and rebuke from Saudi senior officials who attempted to block Plaintiff's website and declared her campaign to be "a crime against the region of Islam" and "an existential threat to Saudi society," *id.* ¶¶ 17, 27.

In or about 2009, the United Arab Emirates ("UAE") contracted with CyberPoint International LLC ("CyberPoint"), a Maryland-based cybersecurity company, to develop a cyber-surveillance program known as "Project Raven." *Id.* ¶ 57. CyberPoint recruited U.S. citizens, including from the National Security Agency and other parts of the U.S. intelligence community, to develop Project Raven. *Id.* CyberPoint's work was governed by U.S. laws and regulations, and employees working on Project Raven were required to obtain proper U.S.

licenses. *Id.* ¶ 59. The licenses permitted CyberPoint to provide defensive cybersecurity services to the UAE, but did not allow it to conduct offensive operations, such as targeting individuals for hacking or cyberattacks. *Id.* ¶ 60.

Defendant DarkMatter is an Emirati company. *Id.* ¶ 6. Beginning in or about December 2015 through February 2016, the UAE transitioned Project Raven from CyberPoint to DarkMatter. *Id.* ¶ 73. Because DarkMatter is not a U.S. company, it was not directly subject to the same U.S. laws as CyberPoint. Under DarkMatter's operation, Project Raven allegedly targeted perceived dissidents of the UAE and Saudi Arabia and hacked their mobile devices. *Id.* ¶¶ 83–86.

Each individual Defendant worked for CyberPoint and DarkMatter, overseeing the development of Project Raven and its transition from CyberPoint to DarkMatter. *Id.* ¶ 73. As part of this transition, the individual Defendants were temporarily assigned or "seconded" to the UAE government's Cyber Intelligence Operations ("CIO") group to carry out Project Raven. Deposition of Samer Khalife, Volume 1, ECF 128-1, Ex. A at 3. During their secondment, they used DarkMatter email addresses, *id.* at 3–4, received employee benefits from DarkMatter, *id.*, and remained working in the same building as before they were seconded, along with the other DarkMatter employees, Deposition of Daniel Gericke, Volume 1, ECF 131-11, Ex. 11 at 18.

Defendant Marc Baier is a U.S. citizen domiciled in the UAE. FAC, ECF 54 ¶ 8. From 2012 to 2015, he worked for CyberPoint and led Project Raven. *Id.* ¶ 62. From about January 2016 to November 2019, he held executive positions at DarkMatter, including as a manager of Project Raven. *Id.* ¶ 8. Defendant Daniel Gericke was a U.S. citizen until February 2017, and on information and belief is now domiciled in Singapore. *Id.* ¶ 9. He worked at CyberPoint in 2013 as a project leader, *id.* ¶ 63, and then began working at DarkMatter in or about October 2015, *id.*

¶ 9. Between about January 2016 and late 2018, Defendant Gericke held senior positions at DarkMatter, including managing and supporting its Computer Network Exploitation operations for Project Raven. *Id.* Defendant Ryan Adams is a U.S. citizen and resident. *Id.* ¶ 10. He worked as a senior software engineer at CyberPoint from 2010 to 2014, *id.* ¶ 64, and then worked for DarkMatter from approximately January 2016 to November 2019, *id.* ¶ 10. At times he served as DarkMatter's Director of Cyber Operations. *Id.*

The individual Defendants allegedly developed hacking systems that allowed Project Raven to gain unauthorized access to protected computers, including computers in the U.S., to allegedly acquire data from perceived dissidents for the UAE. *Id.* ¶ 80.

B. Karma Hacking Tool

One hacking system Defendants developed and deployed was a platform known as "Karma." *Id.* ¶ 92. Karma used a "zero-click" iMessage exploit that took advantage of a vulnerability in Apple's iMessage application to install malware on the target's iPhone and exfiltrate data. *Id.* The zero-click exploits allowed the hacking to remain undetected because the exploit would run without the target having to take any action, such as clicking on a link, navigating to a website, or installing an app. *Id.* ¶ 88. Through the zero-click exploit, hackers could gain access to, collect, delete, modify, or extract data from the device. *Id.* ¶ 89.

Defendant Baier, acting on behalf of DarkMatter, communicated with two U.S. companies to purchase two zero-click iMessage exploits ("Exploit 1" and "Exploit 2") to create Karma and upgrade it to overcome security upgrades to Apple's iOS software. *Id.* ¶ 93. Defendant Baier contracted with one U.S. company to purchase Exploit 1, *id.* ¶¶ 94, 96, which DarkMatter paid for by transferring funds to that company's U.S. bank account, *id.* ¶ 95. All individual Defendants communicated with that company about how to configure Exploit 1 into a hacking system for DarkMatter. *Id.* ¶ 97.

In September 2016, Apple patched vulnerabilities in its operating system, making Exploit 1 less effective. *Id.* ¶ 98. In or about October 2016, Defendant Baier, acting on behalf of DarkMatter, acquired Exploit 2 from a U.S. company. *Id.* ¶ 99. DarkMatter also paid for this exploit by transferring funds to that company's U.S. bank account. *Id.* ¶ 101. As before, the individual Defendants were in direct contact with the U.S. company about how to configure Exploit 2 into a hacking system for DarkMatter. *Id.* ¶ 103.

To enhance Karma's effectiveness, the individual Defendants combined the exploits with other U.S. technology, including computer hardware built in the U.S. *Id.* ¶ 105. Defendants also masked the origin of their hacking transmissions by routing their communications through U.S.-based anonymization services and proxy servers hosted in the U.S. to prevent detection and attribution. *Id.* ¶ 108.

C. Defendants' Alleged Hacking of Plaintiff's iPhone

In late 2017, Plaintiff visited the U.S. to speak at a human rights conference on "Women in the Gulf." *Id.* ¶¶ 28, 143. On November 17, 2017, eleven days before Plaintiff arrived in the U.S., Plaintiff's attendance at the conference was promoted on Twitter. *Id.* ¶¶ 143–44. Plaintiff arrived in the U.S. on November 28, 2017. *Id.* ¶¶ 146, 148. On that day, she announced her arrival in the U.S. on Twitter. *Id.* ¶ 146. On November 30, 2017, Plaintiff spoke at the conference, publicly criticizing the Saudi government's treatment of women. *Id.* ¶ 147.

Plaintiff alleges she brought her iPhone with her to the U.S. while she was there from November 28, 2017 to December 2, 2017, and used it to communicate with friends, family, and other human rights advocates. *Id.* ¶ 148. Plaintiff alleges that Defendants were surveilling her iPhone during this period, *id.* ¶ 143, and that they used Karma's zero-click iOS exploit and associated malware to exfiltrate private data from her iPhone, including her private communications with other human rights advocates, while she was in the U.S., *id.* ¶ 135, 149–

50. Plaintiff alleges that DarkMatter's malware allowed Defendants to view the contents of her device, including data from applications like iMessages, Facebook, and WhatsApp, automatically exfiltrate her data to a server controlled by DarkMatter, and monitor her location and private communications. *Id.* ¶¶ 137–39. During DarkMatter's surveillance of Plaintiff, Plaintiff alleges she was assigned the code name "Purple Sword." *Id.* ¶ 134.

Less than three months later, on March 13, 2018, Plaintiff was allegedly arrested and detained by UAE law enforcement and transported to Saudi Arabia. *Id.* ¶¶ 157–58. In May 2018, Plaintiff was moved to a secret prison in Saudi Arabia where she alleges she was interrogated and tortured. *Id.* ¶ 164. During her interrogation and torture, the interrogators mentioned details about her communications that Plaintiff alleges were obtained by Defendants' hack of her iPhone. *Id.* ¶ 165. Plaintiff was eventually tried along with other female activists. *Id.* ¶ 34. Plaintiff's charging document stated she "was arrested after finding information of her contacting dissidents abroad and what has been found on her social media account by engaging in 'inciting activities.'" *Id.* ¶ 168. The charging document also referenced her communications with human rights advocates and nonprofit organizations located abroad, including in the U.S. *Id.* ¶ 170. Plaintiff alleges Defendants' surveillance of Plaintiff and exfiltration of data on her iPhone through Project Raven facilitated her arrest, detention, and torture. *Id.* ¶ 171.

In 2021, Defendants Baier, Gericke, and Adams entered a Deferred Prosecution Agreement ("DPA") with the National Security Division of the U.S. Department of Justice and the U.S. Attorney's Office for the District of Columbia. *Id.* ¶ 172; DPA, ECF 54-1, Ex. A.[1] The individual Defendants agreed that they had knowingly and willfully conspired to violate, among

[1] The DPA is attached to Plaintiff's FAC, so this Court may assume its contents are true at this stage. *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) (holding that a court may consider "documents attached to the complaint" on a 12(b)(6) motion).

other laws, the Computer Fraud and Abuse Act ("CFAA") during their time at CyberPoint and DarkMatter. FAC, ECF 54 ¶ 173. Under the DPA, the individual Defendants agreed and stipulated to a Factual Statement that described the facts and events underlying their charges. *Id.* ¶ 172; DPA Facts, ECF 54-1, Ex. A.

D. Procedural History

Plaintiff alleges that she discovered DarkMatter had targeted and hacked her phone through reporting by Reuters in late 2019. FAC, ECF 54 ¶ 155. Plaintiff filed suit on December 9, 2021, alleging that all Defendants violated the CFAA, 18 U.S.C. § 1030, and conspired to violate the CFAA, and that the individual Defendants had engaged in the crime against humanity of "persecution on discriminatory grounds." Complaint, ECF 1 ¶¶ 178–234. This Court granted Defendants' first motion to dismiss that complaint for lack of personal jurisdiction but granted Plaintiff leave to amend. ECF 44.

Plaintiff thereafter filed her First Amended Complaint, ECF 54. The FAC adds, among other things, (1) facts about Plaintiff's visit to the U.S. in 2017, (2) allegations that Defendants exfiltrated data from her iPhone while she was physically present in the U.S., and (3) more details about Defendants' acquisition, purchase, and use of U.S.-created exploits, anonymization services, and proxy services from U.S. companies. *Id.*

Following the Ninth Circuit's panel opinion in *Briskin v. Shopify, Inc.*, 87 F.4th 404 (9th Cir. 2023), Plaintiff moved for limited jurisdictional discovery to "assess the nature and extent of Defendants' contacts with" the U.S. ECF 76 at 2. This Court granted Plaintiff's motion but limited the categories of jurisdictional discovery to (1) Defendants' alleged exfiltration of Plaintiff's iPhone data while she was in the U.S. from November 28 to December 2, 2017, and (2) Defendants' contracting with U.S.-based third parties. Opinion and Order, ECF 80 at 4. The parties completed limited jurisdictional discovery, including remote oral depositions of the

individual Defendants, *see* Opinion and Order, ECF 88, on November 14, 2024, *see* ECF 122, 123.

Defendants then filed the instant motions to dismiss. All Defendants move to dismiss the FAC for lack of personal jurisdiction and failure to state a claim under the CFAA. MTD, ECF 126. The individual Defendants separately move to dismiss the ATS claim, which is asserted solely against them. ATS MTD, ECF 127.

On April 21, 2025, after the motions went under advisement, the Ninth Circuit issued its en banc panel decision in *Briskin v. Shopify, Inc.*, 135 F.4th 739 (9th Cir. 2025), which broadened the circumstances in which a court may exercise specific personal jurisdiction over a defendant based on internet-related conduct, including the exfiltration of personal data. This Court requested supplemental briefing from the parties on how that authority alters the personal jurisdiction analysis in this case, ECF 141, which each party filed, Defendants' Supplemental Brief, ECF 142, and Plaintiff's Supplemental Brief, ECF 143. This Court heard oral argument on May 9, 2025. ECF 144.

DISCUSSION

This Court first addresses the threshold issue of personal jurisdiction. *Sinochem Int'l Co. v. Malaysia Int'l Shipping Corp.*, 549 U.S. 422, 430–31 (2007) (holding that "a federal court generally may not rule on the merits of a case without first determining that it has jurisdiction over . . . the parties"). This Court concludes that Plaintiff has alleged facts sufficient at this stage to make a prima facie showing of specific personal jurisdiction over all Defendants. Defendants' allegedly tortious actions deliberately targeted Plaintiff in the U.S. by surveilling her location and private communications and exfiltrating her personal data while she was in the country, including communications with other individuals in the U.S. Defendants also expressly aimed their conduct at the U.S. by using U.S. exploits to commit their tortious actions and using U.S.

anonymization services to avoid detection. Plaintiff has shown her claims arise out of these forum-related contacts. Defendants have not made a compelling case that exercising jurisdiction would be unreasonable, so this Court will exercise personal jurisdiction over all Defendants.

This Court next addresses Defendants' motion to dismiss Plaintiff's CFAA and CFAA conspiracy claims for failure to state a claim under Rule 12(b)(6). This Court concludes that Plaintiff states a valid claim under the CFAA. The text of the CFAA clearly indicates that it is intended to apply extraterritorially, and Plaintiff otherwise adequately pleads facts that support her CFAA claim and satisfy the "damages or loss" requirement. As to the CFAA conspiracy claim, this Court declines to determine, at this stage, that it is barred by the act of state doctrine absent a clear showing that there is a foreign act this Court would have to declare invalid. Defendants' joint motion to dismiss, ECF 126, is accordingly denied.

Finally, this Court turns to the individual Defendants' motion to dismiss Plaintiff's ATS claim for lack of subject-matter jurisdiction. This Court finds that serious foreign policy concerns counsel against recognizing a new ATS cause of action under these circumstances. This Court therefore grants the individual Defendants' motion to dismiss Plaintiff's ATS claim, ECF 127, for lack of subject-matter jurisdiction.

A. Personal Jurisdiction

This Court first outlines the legal standard for personal jurisdiction, then analyzes the three prongs under the minimum contacts test. As explained below, this Court concludes that Plaintiff has made a prima facie showing of specific jurisdiction and Defendants have not met their burden of establishing that exercising personal jurisdiction would be unreasonable.

1. Legal Standard

A court may dismiss a complaint for lack of personal jurisdiction under Federal Rule of Civil Procedure 12(b)(2). "Where a defendant moves to dismiss a complaint for lack of personal

jurisdiction, the plaintiff bears the burden of demonstrating that jurisdiction is appropriate." *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004). Where, as here, "a defendant's motion to dismiss is based on a written record and no evidentiary hearing is held, 'the plaintiff need only make a prima facie showing of jurisdictional facts.'" *Picot v. Weston*, 780 F.3d 1206, 1211 (9th Cir. 2015) (citation omitted). Courts must "resolve[] all disputed facts in favor of the plaintiff" in determining "whether a prima facie showing has been made." *In re W. States Wholesale Nat. Gas Antitrust Litig.*, 715 F.3d 716, 741 (9th Cir. 2013), *aff'd sub nom. Oneok, Inc. v. Learjet, Inc.* 575 U.S. 373 (2015).

Under Federal Rule of Civil Procedure 4(k)(2), "[f]or a claim that arises under federal law," a court may exercise personal jurisdiction over a defendant "not subject to jurisdiction in any state's courts of general jurisdiction" if "exercising jurisdiction is consistent with the United States Constitution and laws." In other words, Rule 4(k)(2) requires three elements: (1) a federal claim, (2) a defendant not subject to personal jurisdiction in any state, and (3) that "the federal court's exercise of personal jurisdiction . . . comport[s] with due process." *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 461 (9th Cir. 2007). Under Rule 4(k)(2), courts "consider contacts with the nation as a whole." *Id.* at 462.

The parties agree that Rule 4(k)(2) governs this action, that Plaintiff asserts exclusively federal claims, and that none of the Defendants are subject to personal jurisdiction in any state's courts of general jurisdiction. MTD, ECF 126 at 6–7 & 7 n.2; Plaintiff's Response in Opposition to Defendants' Second Motion to Dismiss ("Opp'n"), ECF 130 at 12; *see Holland Am. Line*, 485 F.3d at 462 ("[A]bsent any statement from . . . [defendant] that it is subject to the courts of general jurisdiction in another state, the second requirement of Rule 4(k)(2) is met."). The only requirement the parties dispute is whether exercising jurisdiction would be "consistent with the

United States Constitution and laws." Fed. R. Civ. P. 4(k)(2)(B). The only federal law that Defendants identify as limiting this Court's jurisdiction in this case is the Due Process Clause of the United States Constitution. *See* MTD, ECF 126 at 7.

A court may exercise specific personal jurisdiction over a non-U.S. defendant if that defendant has "certain minimum contacts" with the forum "such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice." *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945) (internal quotation marks and citation omitted). A plaintiff must satisfy three elements:

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;
>
> (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and
>
> (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e., it must be reasonable.

CollegeSource, Inc. v. AcademyOne, Inc., 653 F.3d 1066, 1076 (9th Cir. 2011) (quoting *Schwarzenegger*, 374 F.3d at 802). The plaintiff "bears the burden of satisfying the first two prongs." *Id.* If the plaintiff does so, the burden shifts to the defendant at prong three "to set forth a 'compelling case' that the exercise of jurisdiction would not be reasonable." *Id.* (citing *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 476–78 (1985)).

The first prong of the specific jurisdiction test "may be satisfied by purposeful availment, by purposeful direction, or by some combination thereof." *Davis v. Cranfield Aerospace Sols., Ltd.*, 71 F.4th 1154, 1162 (9th Cir. 2023) (internal quotation marks omitted) (quoting *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 433 F.3d 1199, 1206 (9th Cir. 2006) (en banc)). Claims that sound in tort are "typically" analyzed under the purposeful direction test, *id.*,

and claims based on intentional torts are virtually always analyzed under that standard, *see Herbal Brands, Inc. v. Photoplaza, Inc.*, 72 F.4th 1085, 1090 (9th Cir. 2023). Each of Plaintiff's claims require an intentional tortious act. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1196 (9th Cir. 2022) (describing the CFAA as an "anti-intrusion statute" and, relying on legislative history, analogizing a cause of action under the CFAA to tortious "breaking and entering"). This Court accordingly determines that the purposeful direction test applies, ECF 80 at 7, and analyzes that test below. *See Republic of Kazakhstan v. Ketebaev*, No. 17-CV-00246, 2017 WL 6539897, at *5 (N.D. Cal. June 8, 2018) (analyzing CFAA claim under purposeful direction test); *Activision Publ'g, Inc. v. EngineOwning UG*, No. CV 22-0051, 2023 WL 3272399, at *9 (C.D. Cal. Apr. 4, 2023) (same).

2. Purposeful Direction

Courts apply a three-part "effects" test, derived from the Supreme Court's decision in *Calder v. Jones*, 465 U.S. 783 (1984), to evaluate purposeful direction: "the defendant allegedly [must] have (1) committed an intentional act, (2) expressly aimed at the forum state, (3) causing harm that the defendant knows is likely to be suffered in the forum state." *Schwarzenegger*, 374 F.3d at 803 (quoting *Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002)). "An action may be directed at a forum state even if it occurred elsewhere." *Davis*, 71 F.4th at 1163. The analysis "is driven by the defendant's contacts with the forum state—not the plaintiff's or other parties' forum connections." *Id.* (citing *Walden v. Fiore*, 571 U.S. 277, 289 (2014)).

This Court concludes that Plaintiff has made a prima facie showing that Defendants purposefully directed their tortious conduct at the U.S. This Court focuses on the second and

third prongs of the *Calder* effects test: whether Defendants expressly aimed their conduct at the forum and whether they caused foreseeable harm in the forum.[2]

a. Express aiming

The express aiming prong considers a defendant's connection to the forum state and whether the defendant specifically targeted the forum state. *Picot v. Weston*, 780 F.3d 1206, 1214 (9th Cir. 2015). The focus is on the contacts that the defendant creates with the forum, not the unilateral activity of a plaintiff or third party. *Walden*, 571 U.S. at 284–85. The "express aiming" analysis largely depends "on the specific type of tort or other wrongful conduct at issue." *Schwarzenegger*, 374 F.3d at 807.

The alleged torts in Plaintiff's FAC center on Defendants' improper access to and exfiltration of data from Plaintiff's iPhone while she was in the U.S. Plaintiff argues that such conduct, together with Defendants' use of Apple's U.S. servers to transmit the exploit, use of U.S.-based anonymization services and proxy servers to avoid detection, and surveillance of Plaintiff's communications with other individuals in the U.S., combines to satisfy express aiming. Opp'n, ECF 130 at 19–21. Defendants argue neither Plaintiff's voluntary travel to the U.S. nor Defendants' use of U.S.-based servers can satisfy express aiming. MTD, ECF 126 at 10–12.

This Court concludes that Plaintiff has made a prima facie showing that Defendants expressly aimed their conduct at the U.S. by deliberately targeting Plaintiff's iPhone while she was in the U.S. to extract her private communications with other individuals in the U.S.

[2] The parties do not appear to dispute whether Defendants' alleged conduct constituted an intentional act, defined for purposes of the *Calder* test as "an intent to perform an actual, physical act in the real world." *See Schwarzenegger*, 374 F.3d at 806. Defendants' alleged conduct involved intentional acts; hacking, surveilling, and exfiltrating data are acts requiring affirmative conduct.

Defendants' use of U.S. exploits to create their hacking tool and U.S. anonymization services to avoid detection further support a finding of express aiming.

i. Defendants' intentional tortious conduct

Defendants' alleged commission of an intentional tort in the U.S. by exfiltrating data from Plaintiff's iPhone while knowing she was present in the U.S. satisfies express aiming. *See Briskin*, 135 F.4th at 756–57 (holding the defendant's alleged tortious extraction, maintenance, and distribution of California consumers' personal data, while knowing the plaintiffs' devices were in California, satisfied express aiming); *CollegeSource*, 653 F.3d at 1077 (holding express aiming is satisfied "when the defendant is alleged to have engaged in wrongful conduct targeted at a plaintiff whom the defendant knows to be [in] the forum state" (citation omitted)). As several courts have held, express aiming occurs when a defendant accesses a plaintiff's protected computer in the forum to commit a tort.[3]

Still, even when a case involves intentional torts, courts cannot "rely on a defendant's 'random, fortuitous, or attenuated contacts' or on the 'unilateral activity' of a plaintiff." *Walden*, 571 U.S. at 286 (quoting *Burger King Corp.*, 471 U.S. at 475). This Court concludes that neither is the case here.

Defendants make several arguments as to why neither Plaintiff's amended allegations, nor jurisdictional discovery, demonstrate that Defendants deliberately reached into the forum. As

[3] *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 670, 673 n.7 (N.D. Cal. 2020) (holding that "where a defendant enters a forum state with malicious code" and then "commits an intentional tort" in the forum, "such conduct is sufficient to find personal jurisdiction"); *Climax Portable Mach. Tools, Inc. v. Trawema GmbH*, No. 3:18-CV-1825-AC, 2020 WL 1304487, at *7 (D. Or. Mar. 19, 2020) (holding the defendants' intentional tortious accessing of the plaintiff's server in Oregon satisfied express aiming); *Facebook, Inc. v. Sahinturk*, No. 20-CV-08153, 2022 WL 1304471, at *4 (N.D. Cal. May 2, 2022) (holding that the "use of scraping software to send automated commands to Plaintiffs' California-based computers satisfies the 'express aiming' element of the *Calder* 'effects' test").

to Plaintiff's allegations, Defendants argue Plaintiff cannot show that Defendants expressly aimed any conduct at the U.S. because the initial hacking of her device occurred outside the U.S., and then Plaintiff carried her device into the U.S. as it "continuously transmitted data." Defs.' Suppl. Br., ECF 142 at 4. According to Defendants, any alleged exfiltration of data that occurred in the U.S. was not deliberate, but rather was the "the random, isolated, and fortuitous result of Plaintiff's own choice to travel there." *Id.* (citing *Briskin*, 135 F.4th at 758); MTD, ECF 126 at 9–11. Relatedly, Defendants argue that since Plaintiff's hack was "continuous" and because they took no affirmative tortious action against Plaintiff's device while it was in the U.S., this case involves the type of situation foreclosed by *Briskin*'s "traveling cookies" hypothetical and the Supreme Court's opinion in *Walden v. Fiore*, 571 U.S. 277 (2014). Defs.' Suppl. Br., ECF 142 at 4. As to jurisdictional discovery, Defendants argue none of the evidence produced demonstrates that Defendants purposefully directed any tortious conduct at the U.S.; to the contrary, they argue jurisdictional discovery shows Defendants expressly avoided targeting U.S.-based persons or devices. MTD, ECF 126 at 14–16.[4]

[4] Defendants argue the "alleged conduct of the individual Defendants (such as allegations concerning the DPA) may not be attributed to DarkMatter and vice-versa," citing *Rush v. Savchuk,* 444 U.S. 320, 331–32 (1980). MTD, ECF 126 at 6. *Rush* is distinguishable. There, the Supreme Court held a court could not exercise jurisdiction over a defendant who had no forum contacts by way of his insurer's contacts with the forum state, relying on his insurer's contractual obligation to defend and indemnify him. The defendants had no other relationship with each other besides an insured-insurer contractual relationship.

Here, by contrast, the individual Defendants, former senior executives of DarkMatter, have an employee-employer relationship with DarkMatter. As executives, the individual Defendants' contacts with the forum may be attributed to DarkMatter. *Ziegler v. Indian River Cnty.*, 64 F.3d 470, 475 (9th Cir. 1995) ("As its executive vice-president, Richey's contacts are imputed to Riverfront Groves for purposes of determining jurisdiction."); *see also CollegeSource, Inc. v. AcademyOne, Inc.*, 653 F.3d 1066, 1078 (9th Cir. 2011) (attributing "no jurisdictional significance to the fact that [the defendant's] contractor performed the relevant work on [the defendant's] behalf."); *Sher v. Johnson*, 911 F.2d 1357, 1362 (9th Cir. 1990).

This Court concludes that Plaintiff's amended allegations regarding Defendants' alleged intentional exfiltration of data from her iPhone while she was in the U.S. are sufficient to establish express aiming at this stage, and that Defendants' contacts were not random or "mere happenstance." This Court also concludes that none of the evidence produced in jurisdictional discovery sufficiently rebuts Plaintiff's showing of express aiming.

This Court finds this case analogous to the Ninth Circuit's recent en banc opinion in *Briskin v. Shopify, Inc.*, 135 F.4th 739 (9th Cir. 2025). There, the plaintiff Brandon Briskin, a California resident, alleged that the defendant Shopify, a Canadian corporation, violated several California privacy-related tort laws by installing tracking cookies onto his device during an online purchase, allowing Shopify to "extract, collect, maintain, distribute, and exploit" Briskin's personal data for its commercial use. *Id.* at 745–49, 755–56. The en banc panel reversed the prior three-judge panel opinion and held that Shopify's deliberate installation of tracking software onto Briskin's device to extract his personal data satisfied purposeful direction. *Id.* at 756.

Plaintiff's allegations here are factually analogous. The FAC alleges that Defendants installed malware on her iPhone—like the cookies in *Briskin*—that allowed Defendants to exfiltrate location data with the intent of obtaining constant, real-time surveillance of Plaintiff's whereabouts and communications. FAC, ECF 54 ¶ 142. Plaintiff further alleges that based on her social media announcements, Defendants were aware that Plaintiff was speaking at the "Women in the Gulf" conference in Washington D.C. *Id.* ¶ 142–46. Then, with this knowledge and information, Defendants allegedly exfiltrated data from Plaintiff's iPhone while the device was

---

Additionally, Plaintiff's FAC does not improperly lump the individual Defendants and DarkMatter together, but rather explicitly ascribes forum-related conduct to particular Defendants. *Cf. Muertos Roasters, LLC v. Schneider*, No. 22-cv-00051, 2022 WL 3908432, at *2 (E.D. Cal. Aug. 30, 2022) ("Plaintiff may not aggregate factual allegations concerning multiple defendants in order to demonstrate personal jurisdiction over any individual defendant.").

in the U.S., like Shopify's extraction of personal data from consumers that Shopify knew were in California. This Court concludes that Defendants' intentional activities, like Shopify's, constitute express aiming toward the U.S.

This Court disagrees with Defendants that the effect on Plaintiff was random or "mere happenstance." Plaintiff has alleged sufficient facts, construed in the light most favorable to her, that taken together support a strong inference at this stage that Defendants knew Plaintiff's location when they exfiltrated data from her device in the U.S., and thus deliberately targeted her in the U.S. *See Briskin*, 135 F.4th at 756 (holding the effect on Briskin was not "mere happenstance because Shopify allegedly knew the location of consumers like Briskin either prior to or shortly after installing its initial tracking software onto their devices").

Plaintiff publicly campaigned for Saudi women's rights, garnering support from U.S.-based activists and rebuke from the Saudi government, which deemed her campaign "a crime against the region of Islam" and "an existential threat to Saudi society." FAC, ECF 54 ¶¶ 17, 27. Plaintiff alleges her advocacy made her a target of Project Raven, which was designed to target perceived dissidents of the UAE and Saudi Arabia, like herself. Defendants were allegedly surveilling Plaintiff when she and others publicized her public speaking role at a conference in Washington D.C. about women's rights in the Gulf region. Plaintiff spoke at the conference, publicly criticizing the Saudi government's treatment of women. Less than three months later, Plaintiff was allegedly arrested by UAE security services and transferred to a secret prison in Saudi Arabia where she was interrogated and tortured. Plaintiff alleges that during her interrogation, her interrogators mentioned details about her communications that were only available through unlawful access of her device. She also alleges that her Saudi charging

document referenced her private communications on her iPhone, her participation in conferences related to Saudi women's rights, and her contacts with journalists and advocates in the U.S.

Based on these largely uncontroverted allegations and the timing of the events, Plaintiff has made a sufficient showing that Defendants knew Plaintiff was in the U.S. when they allegedly exfiltrated her private communications with U.S. advocates while she was there. *Mohsen v. Morgan Stanley & Co.*, No. CV-13-07358, 2016 WL 9686985, at *5 (C.D. Cal. Mar. 24, 2016), *aff'd*, 710 F. App'x 330 (9th Cir. 2018) ("The Court is not required to turn a blind eye to [p]laintiff's [] pleadings that bear on the plausibility of [p]laintiff's claims."). To carry out Project Raven, Defendants were allegedly tasked with targeting and hacking human rights activists like Plaintiff. Plaintiff was likely on Defendants' radar prior to her visit to the U.S. in November 2017, considering her outspoken opposition to the Saudi government had led the Saudi government to attempt to block her website in the country. Plaintiff's travel to the U.S. was publicized on social media, and the name of the event signaled that its purpose was to advocate for women's rights in the Gulf. Plaintiff was arrested less than three months after her visit to the U.S., and her charging document explicitly mentioned that she was arrested based on information found on her social media account and in her private communications with human rights advocates abroad, including in the U.S. It is reasonable to infer, based on these allegations and the fact that Defendants were allegedly constantly surveilling her location, *see* FAC, ECF 54 ¶ 142, that Defendants knew Plaintiff was in the U.S. when they deliberately exfiltrated data from her device, facilitating her alleged arrest in the UAE and detention in Saudi Arabia.

This case is distinct from *Briskin*'s "traveling cookies" hypothetical and the Supreme Court's opinion in *Walden v. Fiore*, 571 U.S. 277 (2014). The dissent in *Briskin* raised the concern of a "traveling cookie" scenario where once a company attaches geolocation tracking to

a person's electronic device, "jurisdiction attaches wherever that person happens to be" or "happens to travel thereafter." *Briskin*, 135 F.4th at 774 (Callahan, J. dissenting). Invoking *Walden*, the dissent cautioned that this would "impermissibly allow[] a plaintiff's contacts with the defendant and forum to drive the jurisdictional analysis." *Id.* at 756 (quoting *Walden*, 571 U.S. at 289). The majority concluded Shopify's commission of tortious activity "knowing Briskin's device was in California" rendered the traveling cookie hypothetical "inapposite." *Id.* at 756 n.12. Because Shopify knew the device was in California and still committed intentional tortious activity aimed at the device, the court concluded it was properly focused on the relationship among the defendant, the forum, and the litigation, not just where Briskin was located at the time of purchase. *Id.* (citing *Walden*, 571 U.S. at 283–84).

Briskin also distinguished *Walden*, where the plaintiffs were the "only link" between the defendant and the forum. *Id.* at 759. In *Walden*, the plaintiffs were Nevada residents traveling through the Atlanta airport when the defendant, a police officer working as a deputized agent of the Drug Enforcement Administration, seized their allegedly illegitimate cash. 571 U.S. 280–81. After the defendant drafted an affidavit in Georgia to show probable cause for forfeiture of the funds, the plaintiffs filed suit in Nevada for the seizure of their cash and alleging the affidavit was false and misleading. *Id.* at 281. The Supreme Court concluded that the court in Nevada could not exercise personal jurisdiction because the plaintiffs were the "only link" between the defendant and Nevada; "no part of [the defendant's] course of conduct occurred in Nevada." *Id.* at 279, 288–89. In *Briskin*, by contrast, Shopify had other minimum contacts in California, including its installation of software onto devices in California to "continue[] to track their activities." 135 F.4th at 759. The court also noted that *Walden* expressly did not address

situations where intentional torts are committed via the internet or electronically, like in *Briskin*. *Id.*

This Court concludes that the facts here are more like those in *Briskin* than the traveling cookies hypothetical or the facts in *Walden*. Like in *Briskin*, and unlike the defendant in *Walden*, Defendants are alleged to have "deliberately reached out beyond [their] home state by knowingly installing tracking software onto unsuspecting [Plaintiff's iPhone] so that it could later" provide that information to the UAE and Saudi governments, "in a manner that was neither 'random, isolated, [n]or fortuitous.'" *Briskin*, 135 F.4th at 759. Even though Plaintiff voluntarily traveled to the U.S., just as Briskin voluntarily purchased a product online, Defendants still carried out an intentional act aimed at the U.S. by taking the step of exfiltrating data from her iPhone while Defendants knew the iPhone was in the forum. Though the FAC alleges the hack was "continuous and ongoing," FAC, ECF 154 ¶ 150, Defendants retained control over whether data was exfiltrated to a DarkMatter-controlled server, FAC, ECF 154 ¶¶ 126, 129, and Plaintiff alleges Defendants did this when Plaintiff was in the U.S., *id.* ¶¶ 149–50. This deliberate tortious conduct, together with Defendants' other forum-related contacts, explained below, "connects [Defendants] to [the U.S.] in a meaningful way." *Walden*, 571 U.S. at 290.

Finally, jurisdictional discovery does not rebut Plaintiff's prima facie showing of express aiming. Defendants argue that unlike the express aiming in *Briskin*, the individual Defendants testified that the Project Raven CIO group "adhered to a policy of not targeting devices located in the United States." MTD, ECF 126 at 5. According to Defendants, the policy prohibited "exfil[trating] or exploit[ing] any device" that the CIO group "determined . . . was sitting in the United States." Deposition of Daniel Gericke, Volume 2, ECF 128-1, Ex. 7 at 4. Defendants

have not produced any written or documentary evidence of this policy. Absent any corroborating evidence of such a policy, this Court gives this self-serving testimony little weight.

Even if such a policy existed, it confirms—rather than refutes—the fact that Defendants knew devices' locations before targeting them; if they did not know a device's location, they could not follow the policy of avoiding devices based on location. Moreover, Defendants' adherence to any such policy is contradicted by other facts in the record. Defendant Baier testified of at least one occasion of "inadvertent collection" of data from a U.S.-based device. Deposition of Marc Baier, Volume 2 ("Baier Dep., Vol. 2"), ECF 131-10 at 45. And the individual Defendants admit in the DPA that they targeted devices in the U.S. *See* DPA Facts, ECF 54-1, Ex. A ¶ 1 ("The systems developed, maintained, deployed, and operated by Defendants allowed [the CIO group] to gain unauthorized access to, and to thereby acquire data from, computers, electronic devices, and servers around the world, including on computers and servers in the United States . . . in support of the U.A.E.'s intelligence gathering efforts."). Since this Court must resolve jurisdictional factual disputes in Plaintiff's favor at this stage, *see In re W. States Wholesale Nat. Gas Antitrust Litig.*, 715 F.3d 716, 741 (9th Cir. 2013), *aff'd sub nom. Oneok, Inc. v. Learjet, Inc.* 575 U.S. 373 (2015), this Court concludes that even if such a policy existed, Plaintiff has shown at this stage that the individual Defendants did not follow it.

Defendants also argue that "no evidence indicates that the CIO group targeted Plaintiff" and that none of the individual Defendants deposed during jurisdictional discovery "recognized Plaintiff's name or any of her alleged code names." MTD, ECF 126 at 15. This Court does not give this deposition testimony significant weight at this stage because the testimony is internally inconsistent, contradicted by other facts in the record, and inherently self-serving. Defendant Baier testified that although he "was aware of some targets," he could not recall any by name,

see Baier Dep., Vol. 2, ECF 128-1, Ex. 4 at 6, despite having overseen CIO group operations. Defendant Adams testified that he knew targets by name, but also that he did not know whether knowing a target's name would be necessary to target the person. These inconsistencies cast doubt on the veracity of these Defendants' recollections.

These denials are also contradicted by facts in the DPA and the Reuters article,[5] incorporated by reference.[6] Together, these records connect Defendants' conduct to Plaintiff. In the DPA facts, the Defendants admit to targeting devices in the U.S., *see* DPA Facts, ECF 54-1, Ex. A ¶ 1, and the Reuters article identifies Plaintiff as one of their targets, to whom Defendants assigned the code name "Purple Sword." This Court need not credit Defendants' own inherently self-serving testimony, especially since it is contradicted by other facts presented by Plaintiff. *Villiarimo v. Aloha Island Air, Inc.*, 281 F.3d 1054, 1061 (9th Cir. 2002) (holding "uncorroborated and self-serving" testimony did not create a factual dispute).[7]

---

[5] Joel Schectman & Christopher Bing, *White House Veterans Helped Gulf Monarchy Build Secret Surveillance Unit*, Reuters, (Dec. 10, 2019), https://www.reuters.com/article/world/specialreport-white-house-veterans-helped-gulf-monarchy-build-secret-surveillance-idUSKBN1YE1PE/ [https://perma.cc/LJR2-JBA9].

[6] As this Court stated on the record at the May 9, 2025, it would be inappropriate to take judicial notice of the article because it contains facts that are likely disputed. *See* Fed. R. Evid. 201(b). The Reuters article is, however, appropriately incorporated by reference into Plaintiff's FAC, which mentions the article, ECF 154 ¶ 134, and describes that Plaintiff learned of Defendants' alleged hacking through the reporting in the article, *id.* ¶ 155. *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) ("Even if a document is not attached to a complaint, it may be incorporated by reference into a complaint if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim."). This Court "may assume that its contents are true for purposes of a motion to dismiss." *Ritchie*, 342 F.3d at 908.

[7] This Court notes that this testimony also largely goes to the merits of Plaintiff's allegations, which appear to be intertwined with jurisdictional facts. Although the facts alleged in this case require Plaintiff to make a prima facie showing that Defendants knew she was in the U.S. to satisfy express aiming, whether Defendants indeed targeted Plaintiff goes to liability, not jurisdiction. Since "[P]laintiff has made a prima facie showing of jurisdictional facts," it is more appropriate for these merits questions to be decided at a later stage after both parties have had an opportunity to conduct discovery on the merits, so as to avoid prejudicing Plaintiff's case on the

ii. Defendants' use of U.S. exploits and anonymization services to conduct the hacking and avoid detection

Plaintiff's allegations regarding DarkMatter's contacts with U.S. companies further supports this Court's finding that Defendants' conduct was expressly aimed at the U.S. First, Plaintiff alleges Defendants acquired and used U.S.-created exploits to create the Karma hacking system. Second, Plaintiff alleges Defendants targeted and used U.S.-based anonymization services and proxy servers to mask the origin of their hacking. As alleged, none of these contacts is "random, fortuitous, or attenuated."

Defendant DarkMatter argues its "supposed" contacts with various U.S.-based companies, including purchasing exploits used in their hacking system from U.S.-based companies, are insufficient to show DarkMatter directed its conduct at the forum. MTD, ECF 126 at 11–12. Defendants' motion relies heavily on *AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201 (9th Cir. 2020), which the Ninth Circuit recently overruled in its en banc panel opinion in *Briskin*. The court expressly overruled *AMA* "and any other cases that require some sort of different treatment of the forum state for a finding of 'express aiming' of the defendant's allegedly tortious conduct." *Briskin*, 135 F.4th at 758. After *Briskin*, a defendant "'expressly aims' its wrongful conduct toward a forum state when its contacts are its 'own choice and not random, isolated, or fortuitous.'" *Id.* (quoting *Ford Motor Co.*, 141 S. Ct. at 1025).

Here, Defendants' alleged purchase of U.S.-made exploits to incorporate into Karma and use of U.S.-based anonymization services and proxy servers to mask the origin and avoid

---

merits. *Data Disc, Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1289 nn.2, 6–7 (9th Cir. 1977); *see also City & Cnty. of San Francisco v. Purdue Pharma L.P.*, 491 F. Supp. 3d 610, 634 (N.D. Cal. 2020). Since Plaintiff will still have to prove jurisdictional facts at trial by a preponderance of the evidence, *Data Disc, Inc.*, 557 F.2d at 1289 n.2, this Court will permit Defendants to raise these issues on summary judgment or at trial, if appropriate. *See Purdue Pharma*, 491 F. Supp. 3d at 638.

detection are contacts created by Defendants' "own choice" and cannot reasonably be considered random, isolated, or fortuitous.[8] As *Briskin* held, Plaintiff need not show some "forum-specific focus" or similar additional requirement to satisfy express aiming. 135 F.4th at 757. These choices to purchase U.S. exploits from U.S. companies and to use U.S. anonymization services and proxy servers demonstrate Defendants expressly aimed their conduct at the U.S.

Although this Court's prior opinion granting Defendants' first motion to dismiss concluded that "[m]ere knowledge of the location of a third-party's servers . . . is not sufficient to constitute purposeful direction," ECF 44 at 16, Plaintiff's FAC adds allegations that go beyond mere knowledge of the location of a third-party server. *See* FAC, ECF 154 ¶¶ 80–82, 94–103, 105–10. Defendants' choice to use these U.S.-based services for the purpose of masking the origin of their hacking establishes a meaningful connection, *see Will Co. v. Ka Yeung Lee*, 47 F.4th 917, 924 (9th Cir. 2022) (holding that foreign defendants' use of an in-forum server was not fortuitous where "Defendants chose to host the website in Utah"), rather than merely relying on a third party's choice to host their servers in the U.S., *see WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 671 (N.D. Cal. 2020) (finding an out-of-forum defendants' use of an in-forum server was "fortuitous" where "[n]either party controlled where the third parties placed their servers and the servers were not the ultimate target of the intentional act").

[8] Defendants argue that even if DarkMatter had procured technology on behalf of the UAE government entity that allegedly oversaw Project Raven, "it wouldn't have known the purpose or nature of that procurement." MTD, ECF 126 at 15. That DarkMatter did not know the purpose of any allegedly purchased U.S. technology may go to DarkMatter's liability under the CFAA, but it does not go to whether DarkMatter reached into the U.S. This Court will not address Defendants' merits arguments at this stage, especially since Plaintiff has made a prima facie showing of jurisdiction. *See CleanFish, LLC v. Sims*, No. 19-CV-03663, 2020 WL 1274991, at *5 (N.D. Cal. Mar. 17, 2020) ("[W]here the evidence proffered by a defendant merely rebuts a substantive allegation going to the merits of the action, rather than a foundational jurisdictional fact, defendant's evidence cannot nullify the existence of jurisdiction where the plaintiff makes the required prima facie showing.").

b. Foreseeable harm

The final prong of the purposeful direction inquiry requires that Defendants' actions caused harm that would likely be suffered in the forum. *Schwarzenegger*, 374 F.3d at 803. "A defendant causes harm in a particular forum when the 'bad acts' that form the basis of the plaintiff's complaint occur in that forum." *Will Co.*, 47 F.4th at 926 (citation omitted). If a defendant's acts "cause harm in multiple fora, jurisdiction is proper in any forum where a 'sufficient' amount of harm occurs, even if that amounts to only a small percentage of the overall harm caused." *Id.* (citing *Yahoo!*, 433 F.3d at 1207).

This Court concludes that Defendants' alleged actions caused harm that they knew would be suffered in the forum. The bad acts that form the basis of Plaintiff's FAC—Defendants' tortious exfiltration of data—occurred in the U.S., and as explained above, this Court finds that it is reasonable to infer that Defendants knew Plaintiff would be in the U.S. to advocate for women's rights in Saudi Arabia at the time they allegedly exfiltrated her data.

Defendants raise two primary arguments that Plaintiff has not established foreseeable harm. First, they argue no specific bad acts occurred in the U.S. because (1) Plaintiff alleges the hacking occurred before her visit to the U.S., MTD, ECF 126 at 13–14, and (2) the harm to Plaintiff was not "felt" within the forum because Plaintiff learned of the hacking after leaving the U.S. and only suffered the consequences of the hacking after she was detained in the UAE and imprisoned in Saudi Arabia, *id.* at 14. Second, Defendants argue Plaintiff does not allege that they targeted her *because* she would be in the U.S., nor that Defendants actually knew about her trip to the U.S. *Id.* at 12–13. This Court does not find either argument persuasive.

As to Defendants' first argument, this Court concludes that the bad acts that form the basis of Plaintiff's complaint—the surveillance and exfiltration of data from Plaintiff's iPhone—occurred at least in part in the U.S. when Plaintiff was there in late 2017. Even if the hacking

occurred before Plaintiff visited the U.S., Plaintiff alleges that Defendants exfiltrated data from her iPhone, including her private communications, while she was in the U.S. FAC, ECF 54 ¶ 170. The CFAA makes it unlawful to hack "and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). This conduct constitutes a bad act occurring in the forum that forms, in part, the basis of Plaintiff's CFAA claim.

Further, it may be true of Plaintiff's ATS claim that the harm was felt in the UAE and Saudi Arabia, where the harm alleged is Defendants' conspiracy with the UAE to persecute her, leading to her arrest in the UAE and torture in Saudi Arabia. But the harm or injury of Plaintiff's CFAA claim is itself the hacking and exfiltration of data from her iPhone. *See* 18 U.S.C. § 1030(g) (providing a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section"); *see, e.g.*, FAC, ECF 54 ¶¶ 197–98 (alleging Defendants violated 18 U.S.C. § 1030(a)(2)(C) by "access[ing] information" from Plaintiff's iPhone while she was physically present in the U.S., and "as a result of such conduct, caus[ing] damage and loss" (quoting § 1030(a)(5)(C)). As explained above, this conduct occurred at least in part in the U.S. *See Yahoo! Inc.*, 433 F.3d at 1209 (finding harm was felt in the forum, where "significant acts were to be performed" and where "servers that support yahoo.com" were located, even though the defendant may not have desired the effect to be felt in the forum).

As to Defendants' second argument, as this Court explained above, Plaintiff has alleged sufficient facts to support a reasonable inference that Defendants knew Plaintiff would be in the U.S., such that the harm to her device in the forum was foreseeable. Defendants argue Plaintiff's allegation of constant surveillance of Plaintiff's communications with other U.S.-based persons and organizations does not indicate that DarkMatter knew the persons were based in the U.S., nor does it relate to the foreseeability of harm caused to the plaintiff in the forum. MTD, ECF

126 at 13. Plaintiff need not allege that Defendants knew, before reading Plaintiff's exfiltrated private communications, that these *other contacts* were in the U.S. to show Defendants caused harm likely to be suffered in the forum. It is sufficient that Defendants surveilled Plaintiff's iPhone while it was in the U.S. and, upon finding communications with other U.S.-based persons, exfiltrated that data. As stated above, Plaintiff's harm for her CFAA claim was felt in the U.S. where her iPhone was located when Defendants unlawfully accessed and exfiltrated data from it. Taking Plaintiff's allegations as true, Defendants would have known Plaintiff would suffer harm in the U.S. when they hacked and exfiltrated data from her iPhone there.

* * *

In sum, this Court finds that Plaintiff has shown, at this stage, that Defendants purposefully directed their conduct toward the U.S.

3. Whether Claims Arise Out Of or Relate to Defendant's Forum-Related Activities

The second requirement for specific personal jurisdiction is that the plaintiff's claims "must arise out of or relate to the defendant's contacts" with the forum such that there is "an affiliation between the forum and the underlying controversy." *Ford Motor Co.*, 141 S. Ct. at 1025 (citations omitted). For an injury to "arise out of" a defendant's forum contacts, a plaintiff must show "a direct nexus . . . between a defendant's contacts with the forum . . . and the cause of action." *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 504 (9th Cir. 2023). For an injury to "relate to" the defendant's forum contacts, there must be "a close connection between contacts and injury." *Id.* at 506.

This Court concludes that Plaintiff has shown that her claims arise out of Defendants' forum-related contacts. Defendants' forum-related contacts include (1) their alleged tortious exfiltration of data from Plaintiff's iPhone while she was in the U.S. and (2) their acquisition,

use, and enhancement of U.S.-created exploits from U.S. companies to create the Karma hacking tool used to accomplish their tortious conduct. Plaintiff's CFAA claims arise out of these U.S. contacts.

First, "[Plaintiff's] claims 'arise out of' [Defendants'] contacts with [Plaintiff's] device, which [Defendants] allegedly knew was in [the U.S.]" *Briskin*, 135 F.4th at 760. Defendants' "extract[ion] of personal data" from Plaintiff's iPhone in the U.S. "is the kind of contact that would tend to cause privacy injuries." *Id.*[9] This alone satisfies the second requirement for specific jurisdiction.

Second, Plaintiff has also established that her claims arise out of Defendants' use of U.S. exploits to create the Karma hacking tool. *See* Opp'n, ECF 130 at 23–24. The FAC alleges Defendants purchased, used, and enhanced two U.S.-created exploits from U.S. companies to create the Karma hacking tool, ECF 154 ¶¶ 93–111, for the purpose of targeting individuals like Plaintiff, *id.* ¶ 133. The individual Defendants admit they used Karma to hack individuals in the U.S. DPA Facts, ECF 54-1, Ex. A ¶ 59. Defendants' alleged use of Karma to hack Plaintiff's iPhone in the U.S. is sufficient to establish a but-for cause, or "direct nexus," between Plaintiff's CFAA claims and Defendants' forum-related conduct. *Yamashita*, 62 F.4th at 504.[10]

This Court's prior holding that Plaintiff failed to show her claims arose out of or related to Defendants' forum-related contacts was based on the allegations before the Court at that time.

---

[9] Defendants argue these alleged acts "are entirely foreign." Defs.' Suppl. Br., ECF 142 at 5. But Plaintiff's FAC alleges "Defendants exfiltrated private encrypted data from [Plaintiff's] device while she was physically present in the United States." ECF 154 ¶ 150. While the initial installation of the malware occurred abroad, the CFAA also prohibits unlawful exfiltration of data. *See* 18 U.S.C. § 1030(a)(2)(C).

[10] Because this Court concludes that Plaintiff's claims arise out of Defendants' forum-related contacts, Court need not address whether Plaintiff's claims relate to Defendants' contacts.

Those allegations rested largely on Defendants' use of Apple's U.S.-based servers, which this Court concluded would "require[] this Court to impart the affiliation between a third party and the forum to Defendants," which was "foreclosed by the Supreme Court's decision in *Walden v. Fiore*." ECF 44 at 18. Plaintiff has since amended her complaint to include the allegations described above, including Defendants' intentional tortious conduct in the U.S. and purchase of U.S.-created exploits. Plaintiff has also added allegations that Defendants enhanced Karma with other U.S. technology. FAC, ECF 54 ¶ 105. Plaintiff has satisfied this second requirement of specific jurisdiction.

4. Whether Exercising Jurisdiction Would Be Unreasonable

Since Plaintiff has satisfied the first two prongs of the "minimum contacts" analysis, the burden now shifts to Defendants "to set forth a 'compelling case' that the exercise of jurisdiction would not be reasonable." *CollegeSource*, 653 F.3d at 1076. To evaluate reasonableness, courts within the Ninth Circuit use a seven-factor balancing test that weighs:

> (1) the extent of the defendant's purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's state; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Freestream Aircraft (Bermuda) Ltd. v. Aero L. Grp., 905 F.3d 597, 607 (9th Cir. 2018) (citation omitted).

With the benefit of Plaintiff's amended allegations and the completion of jurisdictional discovery,[11] this Court concludes that the factors weigh in favor of holding that the exercise of personal jurisdiction is reasonable.

[11] This Court's prior order on Defendants' first motion to dismiss held that Plaintiff failed to meet the first and second requirements of the minimum contacts analysis, but stated that even

First, this Court finds that Defendants' allegedly tortious conduct presents "purposeful interjection" into the U.S. for the reasons discussed above. *See Ayla, LLC v. Alya Skin Pty. Ltd.*, 11 F.4th 972, 984 (9th Cir. 2021) (holding the purposeful interjection factor is analogous to purposeful direction). "This factor weighs in favor of defendants when the defendant's contacts are attenuated." *X Corp. v. Ctr. for Countering Digital Hate Ltd.*, 724 F. Supp. 3d 921, 944 (N.D. Cal. 2024). As discussed above, Defendants created meaningful contacts with the U.S. Though Plaintiff is a nonresident, Defendants allegedly sought information about her communications with other U.S.-based journalists, human rights activists, and NGOs, thus affecting her affairs within the U.S. *See Ghuman v. Nicholson*, No. CV-20-02474, 2021 WL 673291, at *7 (D. Ariz. Feb. 22, 2021) (finding defendant purposefully interjected into the forum by "repeatedly communicating with individuals that he knew or should have known were [forum] residents in an effort to interfere with the [plaintiff's] personal and economic affairs in [the forum]"). This factor weighs in Plaintiff's favor.

Second, this Court finds that although Defendants would face at least some burden if they were forced to defend the action in the U.S., *see Paccar Int'l, Inc. v. Com. Bank of Kuwait, S.A.K.*, 757 F.2d 1058, 1065 (9th Cir. 1985) (finding jurisdiction unreasonable where a defendant, based in Kuwait, would have to defend a suit in California), this factor ultimately favors Plaintiff. As this Court stated in its prior order, ECF 44 at 20–21, several factors mitigate this burden as to the individual Defendants, all of whom are U.S. citizens who speak, read, and write English. *See Dole Food Co.*, 303 F.3d at 1115. All Defendants are represented by U.S.

---

if Plaintiff had met the requirements, "this Court would still find that the exercise of jurisdiction over Defendants would be unreasonable." ECF 44 at 20. This holding was based on the allegations before the Court at the time, which have been supplemented as described throughout this Opinion.

counsel. *See In re ZF-TRW Airbag Control Units Prods. Liab. Litig.*, 601 F. Supp. 3d 625, 704 (C.D. Cal. 2022) *amended by* 2022 WL 19425927 (noting familiarity with the U.S. legal system and retention of U.S. counsel are mitigating factors in assessing reasonableness). Additionally, all Defendants, including DarkMatter, have been involved in other legal proceedings in the U.S.[12] Finally, the parties' completion of jurisdictional discovery—with each Defendant appearing virtually for two depositions—demonstrates the feasibility of litigating in this forum.

The third factor, the extent of conflict with the sovereignty of the defendant's state, considers "evidence of the [UAE or Saudia Arabia's] particular interest in adjudicating this suit." *Harris Rutsky & Co. Ins. Servs. v. Bell & Clements Ltd.*, 328 F.3d 1122, 1133 (9th Cir. 2003). Though Defendants have not presented evidence of either country's particular interest in adjudicating this suit, this Court is cautious of a potential conflict with either sovereign. *See id.* (presuming a sovereign state had an interest in adjudicating the suit even though no such evidence was presented); *see also Asahi Metal Indus. Co. v. Superior Ct. of California, Solano Cnty.*, 480 U.S. 102, 115 (1987) ("Great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field.").

To be sure, this Court's dismissal of Plaintiff's ATS claim due to possible foreign policy implications lessens the likelihood of a conflict with either sovereign. But the FAC alleges Defendants participated with UAE officials and the Saudi government to facilitate the surveillance, arrest, and detention of Plaintiff. *See* FAC, ECF 54, ¶¶ 47–48, 51, 216–24. Given

[12] The individual Defendants conceded to U.S. jurisdiction when they entered into the DPA. DPA, ECF 54-1, Ex A ¶ 9. DarkMatter appeared in *Oueiss v. Saud*, No. 20-CV-25022, 2022 WL 1311114, at *20 (S.D. Fla. Mar. 29, 2022). Though DarkMatter was dismissed from that case for lack of personal jurisdiction, the court did so under different allegations. *See id.* In that case, unlike this one, the plaintiff did "not claim that she or her mobile device were present in [the forum] when any of the alleged hacks occurred." *Id.*

these allegations, this factor weighs against exercising jurisdiction. That said, the Ninth Circuit has held that "this factor is not dispositive because, if given controlling weight, it would always prevent suit against a foreign national in a United States court." *Gates Learjet Corp. v. Jensen*, 743 F.2d 1325, 1333 (9th Cir. 1984); *see also Harris Rutsky*, 328 F.3d at 1133 ("Although this factor is important, it is not controlling.").

Next, the fourth factor—the forum's interest in adjudicating the dispute—tips in Plaintiff's favor given her amended allegations. Unlike before, where this Court concluded that Defendants should not be hauled into a U.S. court based on "random," "fortuitous," or "attenuated" contacts, ECF 44 at 21–22, Plaintiff has shown that Defendants' contacts were purposefully directed at the U.S. as explained above. The U.S. has a strong interest in protecting against the surveillance and targeting of individuals in the U.S. and the exfiltration of private communications between persons in the U.S. The DPA between the DOJ and the individual Defendants is indicative of the U.S.'s interests in regulating such harm.

Fifth, the U.S. provides "the most efficient judicial resolution of th[is] controversy," *Ayla*, 11 F.4th at 984, which involves claims arising under U.S. law and allegedly tortious conduct that occurred at least in part in the U.S. The amended allegations of Defendants' tortious conduct are no longer "almost completely foreign in nature," as they were when this Court first considered jurisdiction. ECF 44 at 22. Defendants maintain that "any relevant parties, documents, and witnesses are located abroad." MTD, ECF 126 at 23. But as jurisdictional discovery demonstrated, parties and witnesses may appear remotely. *See Harris Rutsky*, 328 F.3d at 1133 (noting that "this factor is 'no longer weighed heavily given the modern advances in communication and transportation" (quoting *Panavision Int'l v. Toeppen*, 141 F.3d 1316, 1323 (9th Cir. 1998)). Plaintiff also identifies several sources of relevant information located in the

U.S. *See* Opp'n, ECF 130 at 26–27. Further, even if some documentary evidence was unobtainable during jurisdictional discovery because it is now controlled by the UAE, *see* MTD, ECF 126 at 23, Plaintiff "will be able to access evidence for her claims by proceeding to merits discovery and seeking information from U.S. third parties, which was beyond the scope of jurisdictional discovery." Opp'n, ECF 130 at 27.

The sixth factor—the importance of the forum to the plaintiff's interest in convenient and effective relief—weighs in Plaintiff's favor. Plaintiff brings her claims under U.S. law, which heightens Plaintiff's interest in her claims being adjudicated by a U.S. court. The seventh factor—the availability of an alternative forum—also favors jurisdiction. Plaintiff alleges the UAE targets activists, such as Plaintiff, by using Defendants' technology to hack her device and surveil her movements and communications, to ultimately intimidate and harass. *See* FAC, ECF 54 ¶¶ 37, 83, 140. These allegations demonstrate that the UAE would likely be a hostile forum to Plaintiff's claims.

In sum, all factors but three and five weigh in favor of exercising jurisdiction, and neither of those factors is given dispositive weight. This Court therefore finds that Defendants have not met their burden of setting forth a "compelling case" that exercising jurisdiction would be unreasonable. This Court will exercise personal jurisdiction over all Defendants.

B. CFAA and Conspiracy Claims

Plaintiff alleges two CFAA claims against all Defendants: (1) violations of the CFAA, and (2) conspiracy to violate the CFAA. Defendants move to dismiss both. MTD, ECF 126 at 26. Addressing each claim in turn, this Court first concludes that Plaintiff adequately pleads a violation of the CFAA. The text of the CFAA clearly indicates that it applies extraterritorially. Defendants' argument to the contrary inappropriately divorces the definition of "protected computer" from the underlying violations. Plaintiff also adequately pleads facts supporting her

CFAA claim and satisfies the "damages or loss" requirement. The Defendants' motion to dismiss Plaintiff's CFAA claim is denied.

As to Plaintiff's CFAA conspiracy claim, this Court does not conclude, at this stage, that it is barred by the act of state doctrine absent a clear showing that there is a foreign act this Court would have to declare invalid. Defendants have not made this showing, so their motion to dismiss the CFAA conspiracy claim is denied.

1. Legal Standard

Federal Rule of Civil Procedure 12(b)(6) provides that a court may dismiss a complaint for failing to state a claim upon which relief can be granted. "To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 554, 570 (2007)). The court must construe all well-pleaded material facts in the light most favorable to the non-moving party. *Rowe v. Educ. Credit Mgmt. Corp.*, 559 F.3d 1028, 1029–30 (9th Cir. 2009). Uncontroverted allegations in the complaint must be taken as true. *Boschetto v. Hansing*, 539 F.3d 1011, 1015 (9th Cir. 2008). However, a court need not accept as true "[t]hreadbare recitals of a cause of action's elements, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678.

2. CFAA Claim

The CFAA "prohibits a number of different computer crimes, the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130–31 (9th Cir. 2009). To state a claim under the CFAA, a plaintiff must allege that the defendant "violated one of the provisions of § 1030(a)(1)-(7)." *Id.* Plaintiff alleges that Defendants violated § 1030(a)(2)(C) by

accessing her phone and exfiltrating data without authorization, FAC, ECF 54 ¶¶ 186–87, and violated § 1030(a)(5)(A), § 1030(a)(5)(B), and § 1030(a)(5)(C) by transmitting malware to her phone that impaired the phone's data integrity and security systems, *id.* ¶¶ 188–99.

To bring a civil action under the CFAA, a plaintiff must also show that she (1) "suffer[ed] damage or loss by reason of [the defendant's] violation" of the CFAA, and (2) that one of the five enumerated circumstances in § 1030(c)(4)(a)(i) is present. As relevant to this case, the second element is met when the CFAA violation caused at least $5,000 in damages, § 1030(c)(4)(A)(i)(I), or "physical injury to any person," § 1030(c)(4)(A)(i)(III). Plaintiff alleges that she incurred at least $5,000 in damages in responding to the hack and attempting to restore her data, FAC, ECF 54 ¶¶ 204–11, and that she suffered physical injury as a result of the hack, *id.* ¶¶ 212–14.

Defendants move to dismiss the CFAA claim on three grounds. First, as a preliminary issue, they argue that the CFAA does not apply extraterritorially. MTD, ECF 126 at 26–28. Second, they argue that Plaintiff fails to allege facts sufficient to show a violation of the CFAA. *Id.* at 28–29. Finally, they argue that Plaintiff has failed to meet the statutory "damages or loss" requirement. *Id.* at 29–32. This Court rejects all of these arguments.

a. Extraterritoriality

Defendants argue Plaintiff seeks an impermissible extraterritorial application of the CFAA because (1) her iPhone does not qualify as a "protected computer" within the meaning of the statute and (2) the CFAA does not apply to foreign conduct. MTD, ECF 126 at 26–27. Addressing the second argument first, this Court concludes that the CFAA applies extraterritorially. This Court also finds that Plaintiff pleads an adequate nexus between her phone and the U.S. to qualify as a "protected computer" under the CFAA.

i. The CFAA applies extraterritoriality

"It is a longstanding principle of American law that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States." *Abitron Austria GmbH v. Hetronic Int'l, Inc.*, 143 S. Ct. 2522, 2528 (2023) (citation omitted). The Supreme Court has established a two-step framework for analyzing questions of extraterritoriality. *See id.* The first step asks whether "Congress has affirmatively and unmistakably instructed that the provision at issue should apply to foreign conduct." *Id.* (citation omitted). If so, claims alleging foreign conduct may proceed; if not, step two asks "whether the suit seeks a (permissible) domestic or (impermissible) foreign application of the provision." *Id.*

At step one, a "dispositive" indication of extraterritorial reach may come from a statute's context. *RJR Nabisco v. European Cmty.*, 579 U.S. 325, 337 (2016). While Congress must provide "a clear indication of extraterritorial effect," it need not include an "express statement of extraterritoriality." *Id.* The presumption against extraterritoriality is a "canon of construction," not "a limit upon Congress's power to legislate." *Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010).

This Court concludes at step one that "the text of the CFAA provides a clear indication of extraterritorial application." *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 449 (N.D. Cal. 2018), *reconsideration granted on other grounds*, 386 F. Supp. 3d 1155 (N.D. Cal. 2019). The statute lists offenses that occur when a defendant unlawfully accesses a "protected computer," which is defined to include a computer "used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). This definition is "as clear an indication [of extraterritorial application] as possible short of saying 'this law applies abroad.'" *In re Apple*, 347 F. Supp. 3d at

448 (quoting *Ryanair DAC v. Expedia Inc.*, No. C17-1789, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018)).

Every court to consider the question has concluded that the CFAA applies extraterritorially. *See In re Apple*, 347 F. Supp. 3d at 448; *Ryanair*, 2018 WL 3727599, at *2; *Ryanair DAC v. Booking.com B.V.*, No. 20-1191, 2025 WL 266631, at *7 (D. Del. Jan. 22, 2025); *United States v. Ivanov*, 175 F. Supp. 2d 367, 375 (D. Conn. 2001); *see also United States v. Gasperini*, 729 F. App'x 112, 114 (2d Cir. 2018) (noting that "[t]here is a strong argument that § 1030(a)(2) applies extraterritorially"). This conclusion aligns with the CFAA's definition of a "government entity" as including "any foreign country, and any state, province, municipality, or other political subdivision of a foreign country," *see Ivanov*, 175 F. Supp. 2d at 374 (citing 18 U.S.C. § 1030(e)(9)), and the CFAA's legislative history, which shows a clear understanding that the law would reach individuals based outside of the U.S. who hacked U.S.-based computers, *see* S. Rep. No. 104-357, 1996 WL 492169, at *4 (1996).

Defendants argue that the CFAA's reference to certain foreign devices does not mean it also applies to foreign conduct, suggesting the provision may be read only to extend to a "domestic hacker" who "target[s] a foreign device." MTD, ECF 126 at 28. Aside from cases about the presumption against extraterritoriality generally, Defendants cite no case in support of this theory.

This Court rejects this narrow reading of the CFAA, which divorces the definition of "protected computer" from the rest of the statute. Each of the substantive subsections of § 1030(a) "guard[s] against harm, damage, or unauthorized access to a 'protected computer.'" *Ryanair*, 2018 WL 3727599, at *2. In defining "protected computer" to apply extraterritorially, Congress intended the provisions incorporating that phrase to also apply extraterritorially; if not,

the definition would have no meaning. This reading of CFAA's plain language also aligns with its legislative history, which shows that Congress was concerned that the prior version of the statute did not extend to "computers used in foreign communications or commerce, despite the fact that hackers are often foreign-based." S. Rep. No. 104-357, 1996 WL 492169, at *4.

This Court agrees with the reasoning in *Ryanair* that it "would make little sense" to hold CFAA's civil provision does not apply extraterritorially "given the *conduct* the CFAA regulates." 2018 WL 3727599, at *2–3 (emphasis added). The CFAA regulates unauthorized computer access and transmission that happens "simultaneously at the locations of the accessor and the accessed computer" through "servers around the globe." *Id.* at *3. By nature of the conduct the CFAA regulates, it would obviate the statute's application to foreign devices if it were limited to purely domestic conduct by a defendant. And as the court in *Ryanair* points out, the requirement that Plaintiff establish that the Court has personal jurisdiction over Defendants serves as a limit on CFAA claims involving foreign parties and a foreign device. *Id.* at *3 n.3.

ii. The scope of the CFAA's extraterritorial application

That a statute applies extraterritorially is only half the analysis. Once a court concludes that a statute applies extraterritorially, the scope of its extraterritorial application "turns on the limits Congress has (or has not) imposed" in the statutory text. *RJR Nabisco*, 579 U.S. at 337–38. Defendants argue that the statutory term "protected computer" limits the extraterritorial scope of the statute by requiring "a substantial nexus between [Plaintiff's] phone and the United States," pointing out that the statute would otherwise "reach almost any hack occurring anywhere in the world." MTD, ECF 126 at 27.

"The term 'protected computer' refers to . . . effectively any computer connected to the Internet." *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 (9th Cir. 2022). Courts have routinely found that Internet-connected computers, wherever they may be located, are part "of a

system that is inexorably intertwined with interstate commerce." *United States v. MacEwan*, 445 F.3d 237, 245 (3d Cir. 2006). This definition "sweeps broadly" and thus "does not serve as the CFAA's main limiting principle." *United States v. Yücel*, 97 F. Supp. 3d 413, 419 (S.D.N.Y. 2015). That breadth has not stopped courts from embracing a definition of "protected computer" that extends to all Internet-connected devices. *See id.* at 418 (collecting cases); *Ivanov*, 175 F. Supp. 2d at 374 (reading the term to apply "to computers used *either* in interstate *or* in foreign commerce" (emphasis added)).

Defendants are correct, however, that the definition is limited to computers "used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). The CFAA thus "does not apply extraterritorially in all cases involving a computer." *Ryanair*, 2025 WL 266631, at *6. Rather, the use of the phrase "affecting interstate or foreign commerce" indicates that Congress "is exercising its full power under the Commerce Clause," *Yücel*, 97 F. Supp. 3d at 419, up to the limits of that Clause.

The Foreign Commerce Clause confers "sweeping powers over foreign commerce," *United States v. Clark*, 435 F.3d 1100, 1109 (9th Cir. 2006), and Defendants do not squarely argue that the CFAA's application to this case would be unconstitutional. *See United States v. Park*, 938 F.3d 354, 374 (D.C. Cir. 2019) (describing the exact boundaries of Congress's foreign commerce powers as "judicially unexplored"). This Court agrees with Defendants' suggestion that some sort of effects test likely defines the outer parameters of the Clause, and thus the outer parameters of CFAA liability. *See* MTD, ECF 126 at 27 (contending the statute should be read to require a "substantial nexus"); *In re Sealed Case*, 936 F.3d 582, 591 (D.C. Cir. 2019). This Court also agrees with Defendants that "[a] random Internet connection in Saudi Arabia or the UAE—without more—does not 'directly involv[e]' the United States." Reply, ECF 135 at 23.

Precedent from this Circuit, however, requires only a "constitutionally tenable nexus with foreign commerce" to fall within Congress's Foreign Commerce Clause power. *Clark*, 435 F.3d at 1114. A plaintiff may meet that burden at this stage by alleging that his or her device is used in foreign commerce or communication with the United States. *See In re Apple Inc.*, 347 F. Supp. 3d at 449. As described above in this Court's findings on jurisdiction, Plaintiff alleges she used her device to communicate with people in the U.S., FAC, ECF 54 ¶ 149, that she used it to make communications while physically present in the U.S., *id.*, and that Defendants exfiltrated data from her iPhone while it was in the U.S., *id.* ¶ 150. These communications provide a "tenable nexus" with the United States that distinguishes Plaintiff's phone from a "random Internet connection in Saudi Arabia or the UAE," which is sufficient to plead her iPhone was a protected computer under the CFAA.

b. Sufficiency of pleaded facts

Defendants argue Plaintiff's amended allegations "do not plausibly link any Defendant to the alleged unauthorized access" of Plaintiff's iPhone, but rather are conclusory and speculative allegations that Defendants were connected to the hacking. MTD, ECF 126 at 28. Construing Plaintiff's allegations in the light most favorable to her, this Court finds that Plaintiff has pled sufficient facts connecting Defendants to the alleged hacking and exfiltration of data from her iPhone.

As to DarkMatter, Plaintiff alleges that, "[o]n information and belief, DarkMatter operatives hacked [Plaintiff's] iPhone by targeting her as a recipient of the 'zero-click' iOS exploit and malware," and that once the malware was embedded on Plaintiff's iPhone, Defendants exfiltrated data to a DarkMatter server. FAC, ECF 54 ¶¶ 135–36, 139. The FAC also alleges DarkMatter purchased the U.S. exploits used to create the hacking tool, Karma, that operatives used to carry out their tortious activities. *Id.* ¶¶ 80–82, 94–103. In addition, the

Reuters article incorporated by reference explains DarkMatter's offensive cyber-security programs for the UAE and reports on DarkMatter's role in targeting Plaintiff.[13] These allegations are sufficient to connect DarkMatter to her CFAA and CFAA conspiracy claims.

Defendants take issue with Plaintiff's "information and belief" allegations, characterizing them as "speculative" or "unsupported by specific facts connecting DarkMatter to the alleged hack." MTD, ECF 126 at 28. The Ninth Circuit has held that plaintiffs may plead facts alleged upon information and belief "where the facts are peculiarly within the possession and control of the defendant." *Soo Park v. Thompson*, 851 F.3d 910, 928 (9th Cir. 2017) (quoting *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 120 (2d Cir. 2010)). If ever there was a case when information regarding a defendant is not reasonably available to a plaintiff, this is the one. As Defendants themselves represented throughout jurisdictional discovery, much of the information Plaintiff sought regarding DarkMatter no longer exists. *See* DarkMatter's Answers to Written Deposition Questions, ECF 131-8 at 15 ("[N]o DarkMatter documents, other than those necessary to wind down the company, exist."); Letter from DarkMatter's counsel to Plaintiff's counsel, ECF 131-16 at 1 ("[DarkMatter] is not in possession of corporate records from the period of time during which DarkMatter was active . . . other than certain accounting documents."). What does exist is likely "subject to foreign [Emirati] government control." MTD, ECF 126 at 23. If DarkMatter, an Emirati company that allegedly seconded its employees—including the individual Defendants—to an Emirati agency, cannot obtain relevant information underpinning Plaintiff's claims, then surely such information would not be reasonably available

[13] Joel Schectman & Christopher Bing, *White House Veterans Helped Gulf Monarchy Build Secret Surveillance Unit*, Reuters, (Dec. 10, 2019), https://www.reuters.com/article/world/specialreport-white-house-veterans-helped-gulf-monarchy-build-secret-surveillance [https://perma.cc/LJR2-JBA9].

to Plaintiff. This is especially true if, as Plaintiff alleges, the UAE works closely with Saudi Arabia to target perceived dissidents, FAC, ECF 54 ¶¶ 47–48, 51, and Saudi Arabia views Plaintiff and her women's rights activism as an "existential threat to Saudi society," *id.* ¶ 27.

As to the individual Defendants, the FAC attaches the Deferred Prosecution Agreement, which contains a comprehensive set of facts to which the individual Defendants agreed and admitted. ECF 54-2, Ex. B. These facts establish the individual Defendants operated Karma to target and hack a class of victims to which Plaintiff belongs: perceived dissidents of the UAE and Saudi Arabia. While the DPA does not mention Plaintiff or any individual victim by name, the Reuters article *does* connect Plaintiff to the conduct Defendants admitted to in the DPA. FAC, ECF 54 ¶ 134. Plaintiff alleges that public reporting by Reuters, based on interviews with whistleblowers who previously worked on Project Raven and an independent review of Project Raven documents, revealed that Project Raven used a platform known as Karma to hack into the iPhones of "hundreds of activists." *Id.* ¶ 133. This included using Karma to obtain photos, emails, text messages, and location information from targets' iPhones during 2016 and 2017. *Id.* Later reporting by Reuters revealed that Defendants assigned Plaintiff the codename "Purple Sword" and targeted her in 2017. *Id.* ¶ 134. This Court finds these allegations "are sufficiently particular and detailed to indicate their reliability." *In re Wet Seal, Inc. Sec. Litig.*, 518 F. Supp. 2d 1148, 1172 (C.D. Cal. 2007) (citation omitted); *see In re McKesson HBOC, Inc. Sec. Litig.*, 126 F. Supp. 2d 1248, 1272 (N.D. Cal. 2000) (stating that courts may credit newspaper articles that include "numerous factual particulars" and are "based on an independent investigative effort").

c. Damage or loss requirement

The CFAA authorizes a civil claim when a person "suffers damage or loss by reason of a [CFAA] violation," 18 U.S.C. § 1030(g), and one of the five enumerated circumstances in

§ 1030(c)(4)(a)(i) is present. Plaintiff relies on the first circumstance, "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value," § 1030(c)(4)(A)(i)(I), and the third circumstance, "physical injury to any person," § 1030(c)(4)(A)(i)(III). Defendants argue Plaintiff fails to state a claim satisfying either. MTD, ECF 126 at 29–32. This Court concludes Plaintiff has sufficiently alleged damage or loss pursuant to 18 U.S.C. § 1030(g) under a loss of at least $5,000, so this Court need not address her physical injury damage or loss allegations.[14]

The FAC alleges Plaintiff "suffered loss aggregating at least $5,000 in value . . . due to responding to the hack, conducting a damage assessment, and attempting to restore data." ECF 54 ¶ 203. Specifically, she alleges she spent at least 100 hours responding to the hacks, including: (i) communicating with cyber-security experts about the hack and contacting other individuals whose information may have been intercepted by Defendants, (ii) developing new security protocols, and (iii) "remaining informed about the latest threats against her digital security." *Id.* ¶ 204. She also alleges that due to the hack, she "has had to employ new security

[14] This Court notes that Plaintiff likely adequately alleges physical injury under the CFAA. The FAC alleges that Plaintiff suffered physical injury because of Defendants' hack and surveillance, which led to her arbitrary detention by the UAE and her imprisonment and torture in Saudi Arabia. ECF 54 ¶¶ 185, 212. Even if the CFAA requires a proximate causal relationship between the unauthorized access and the physical injury, as Defendants argue, *see* MTD, ECF 126 at 31–32, the Saudi forces' alleged acts were likely a foreseeable result of Defendants' alleged CFAA violations. *See Farr v. NC Machinery Co.*, 186 F.3d 1165, 1169 (9th Cir. 1999) (holding an intervening or superseding cause does not relieve an earlier actor of liability if it was foreseeable). Plaintiff alleges Project Raven's purpose was to identify human rights activists like Plaintiff, FAC, ECF 54 ¶ 83, Defendant Baier admitted the Project Raven team was "supporting the UAE government," Baier Dep., Vol. 2, ECF 131-10 at 21, and Plaintiff alleges that some of the information Defendants exfiltrated from her iPhone was mentioned in her Saudi charging documents. *Id.* ¶ 170. As argued by Plaintiff, the FAC has alleged sufficient facts from which it can be reasonably inferred that Defendants' alleged CFAA violations facilitated the Saudi forces' conduct, such that Plaintiff's physical injuries "flow[ed] directly," Reply, ECF 135 at 28, from Defendants' violations.

measures to protect the confidentiality of her communications, which has impaired her ability to carry out her human rights work." *Id.* ¶ 205.

Defendants argue these loss allegations "merely track the statutory standard" and "do not support an inference that Plaintiff incurred $5,000 in costs." MTD, ECF 126 at 30–31. Specifically, Defendants argue Plaintiff does not allege she paid the cyber-security experts she communicated with "or that she made any expenditures at all," and does not quantify the value of the time she spent responding to the hack or the impairment to her human rights work. MTD, ECF 126 at 30.

The CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense." § 1030(e)(11). This definition is limited to "harms caused by computer intrusions, not general injuries unrelated to the hacking itself." *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 (9th Cir. 2019). Defendants do not dispute that the costs identified above fall within this statutory definition,[15] but contend that the allegations are insufficient to meet the $5,000 requirement. MTD, ECF 126 at 30.

Plaintiff's allegations are sufficient at this stage for this Court to plausibly infer that Plaintiff's "loss" exceeds $5,000. Courts in the Ninth Circuit do not require plaintiffs to allege the type of detailed cost itemizations Defendants suggest. For example, in *Ticketmaster L.L.C. v. Prestige Entertainment West, Inc.*, the court concluded that the plaintiff's allegations of "a panoply of costs necessitated by [the d]efendants' unauthorized access, including the costs of . . . expanding security to identify and block bots . . . and hiring of third-party consultants to

[15] Because this Court finds that Plaintiff sufficiently alleges "loss" based on the costs of responding to the hack, it need not address whether Plaintiff's alleged "other compensatory damages," FAC, ECF 54 ¶¶ 206–11, fall within the CFAA's definition of "loss."

implement additional bot mitigation measures," were sufficient to infer "loss" exceeding $5,000. 315 F. Supp. 3d 1147, 1173 (C.D. Cal. 2018). Similarly, in *Meta Platforms, Inc. v. BrandTotal Ltd.*, the court accepted a cost estimate based "entirely on [plaintiff's] own internal investigation costs." 605 F. Supp. 3d 1218, 1263 (N.D. Cal. 2022). Plaintiff's allegation that she spent at least 100 hours investigating and responding to the actual damage to her phone caused by the hack suffices to allege loss. *See Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) (the fact that the plaintiffs "spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to [the defendant's] actions" showed they suffered a loss under the CFAA); *see also Meta Platforms*, 605 F. Supp. 3d at 1265 (reaffirming the validity of losses based on "investigative costs").

The allegations in Plaintiff's FAC, like those in *Ticketmaster*, can be contrasted with the case Defendants cite in support of their argument, where the plaintiff did not offer a dollar figure and instead only alleged an entitlement "to recovery of such damages as alleged herein or as may be provided under the statutory violation alleged." *Brooks v. Agate Res., Inc.*, No. 6:15-CV-00983-MK, 2019 WL 2635594, at *24 (D. Or. Mar. 25, 2019), *report and recommendation adopted*, 2019 WL 2156955 (D. Or. May 14, 2019). That court held that the plaintiff had not sufficiently pleaded a loss of at least $5,000. *Id.* Here, by contrast, Plaintiff alleges that she suffered at least $5,000 in costs specifically in responding to Defendants' unauthorized access. FAC, ECF 54 ¶ 203. While this Court need not credit conclusory allegations that recite one of the elements of a cause of action, *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009), Plaintiff also provides factual allegations to support this valuation. *See id.* ¶¶ 204–05. This Court finds it plausible, drawing reasonable inferences in Plaintiff's favor, that the costs alleged could meet the $5,000 threshold. To the extent Defendants raise factual disputes as to whether Plaintiff

appropriately valued her time or that of the cyber-security experts with whom she corresponded, those disputes are properly considered at a later stage of the litigation.

3. CFAA Conspiracy Claim

Defendants argue Plaintiff's CFAA conspiracy claim should be dismissed because (1) Plaintiff's standalone CFAA claim fails, so the conspiracy claim does too, and (2) the act of state doctrine precludes the conspiracy claim. Because this Court concludes that Plaintiff states a valid CFAA claim, it only addresses Defendants' act of state doctrine argument.

The act of state doctrine is a "rule of decision" that requires that "the acts of foreign sovereigns taken within their own jurisdictions shall be deemed valid." *W.S. Kirkpatrick & Co. v. Env't Tectonics Corp., Int'l*, 493 U.S. 400, 405, 409 (1990). The doctrine "reflect[s] 'the strong sense of the Judicial Branch that its engagement in the task of passing on the validity of foreign acts of state may hinder' the conduct of foreign affairs." *Id.* at 404 (citation omitted). "In its modern formulation, the doctrine bars suit where '(1) there is an official act of a foreign sovereign performed within its own territory; and (2) the relief sought or the defense interposed in the action would require a court in the United States to declare invalid the foreign sovereign's official act.'" *Sea Breeze Salt, Inc. v. Mitsubishi Corp.*, 899 F.3d 1064, 1069 (9th Cir. 2018) (quoting *W.S. Kirkpatrick*, 493 U.S. at 409) (cleaned up).

Plaintiff's FAC alleges that Defendants engaged in a conspiracy with "UAE officials" to violate the CFAA. ECF 54 ¶ 216. Specifically, Plaintiff alleges that the individual Defendants, as employees of CyberPoint, "reached an actual or tacit agreement with each other, and with UAE officials and DarkMatter, to transfer U.S. technology and knowhow . . . to DarkMatter for the purpose of implementing Project Raven's hacking protocols and gaining unauthorized access to protected computers." *Id.* ¶ 219. Plaintiff alleges "Defendants carried out their hacks against targets identified by UAE officials and knowingly facilitated the transfer of information collected

from their hacks to UAE officials." *Id.* ¶ 221. And Plaintiff alleges Defendants committed several overt acts in furtherance of this conspiracy. *Id.* ¶¶ 222–24.

The first element of the act of state doctrine—an official act of a foreign sovereign performed within its own territory—is met. Plaintiff alleges Defendants conspired with "UAE officials" to violate the CFAA. The acts of these officials "can be considered the acts of the foreign state," *Samantar v. Yousuf*, 560 U.S. 305, 322 (2010), and Plaintiff alleges the purported conspiracy occurred in the UAE, *see* FAC, ECF 54 ¶¶ 55–86, 218–24. Plaintiff's opposition brief does not dispute that this element is met, so she has waived any argument to the contrary. *E.E.O.C. v. PC Iron, Inc.*, 316 F. Supp. 3d 1221, 1230 (S.D. Cal. 2018) (argument not disputed in an opposition brief is waived).

The parties primarily dispute the second element—whether adjudicating this action would require this Court to declare invalid a foreign sovereign's official act. Defendants argue that for Plaintiff to prevail, this Court "would have to conclude that the UAE government and Defendants agreed to act unlawfully in the UAE's territory." MTD, ECF 126 at 32. Plaintiff contends her CFAA conspiracy claim does not challenge "the validity of a domestic official act by the UAE," but rather "whether Defendants—non-state actors—violated U.S. law." Opp'n, ECF 130 at 35.

Defendants misapprehend the breadth and application of the act of state doctrine. The doctrine is a "principle of decision" that looks to "the relief sought or the defense interposed." *W.S. Kirkpatrick*, 493 U.S. at 405–06. It applies only "when the outcome of the case turns upon . . . the effect of official action by a foreign sovereign." *Id.* at 406.

The doctrine thus applies when, for example, adjudicating a claim will require invalidating the decision of a foreign court, *Von Saher v. Norton Simon Museum of Art at*

Pasadena, 897 F.3d 1141, 1152 (9th Cir. 2018), declaring a permit denial wrongful, *World Wine Minerals, Ltd. v. Republic of Kazakhstan*, 296 F.3d 1154, 1165 (D.C. Cir. 2002), assessing the expropriation of property, *id.* at 1166, or evaluating a foreign sovereign's compliance with its own laws, *Royal Wulff Ventures LLC v. Primero Mining Corp.*, 938 F.3d 1085, 1093 (9th Cir. 2019). Each of these cases would have required the court to determine the validity of the foreign sovereign's acts. But the doctrine "does not preclude courts from imposing extraterritorial legal consequences arising from [a foreign sovereign] act in accordance with applicable law." *Petróleos de Venezuela S.A. v. MUFG Union Bank, N.A.*, 51 F.4th 456, 467 (2d Cir. 2022).

This Court concludes that the act of state doctrine does not bar this Court from assessing whether the Defendants here conspired to violate U.S. federal law.[16] *See* FAC, ECF 54 at 50. It is unclear from Defendants' briefing what foreign official act they believe Plaintiff is asking this Court to declare invalid. Resolving Plaintiff's claim will not have any "direct effect on any official declaration, decree, law, or act" of the UAE. *Sharon v. Time, Inc.*, 599 F. Supp. 538, 546 (S.D.N.Y. 1984). Even if some factual findings may "cast doubt upon the validity of foreign sovereign acts," liability under the CFAA turns on whether the acts alleged in Plaintiff's FAC occurred, not whether they were valid under Emirati law. *See W.S. Kirkpatrick*, 493 U.S. at 406. As in *Kirkpatrick*, Plaintiff is "not trying to undo or disregard governmental action," and therefore may "obtain damages from [the] private parties" she seeks to hold liable under U.S. law. 493 U.S. at 407 (citing *United States v. Sisal Sales Corp.*, 274 U.S. 268, 276 (1927)). Nothing in Plaintiff's conspiracy claim rests on the proposition that any act of the UAE or its officials was invalid.

[16] This Court acknowledges that it likely lacks personal jurisdiction against the unnamed UAE officials, and would likely be unable to award any relief against them. *See Samantar*, 560 U.S. at 311–12.

C. Subject Matter Jurisdiction Over ATS Claim

Defendants Marc Baier, Ryan Adams, and Daniel Gericke move under Federal Rule of Civil Procedure 12(b)(1) to dismiss Plaintiff's claims under the Alien Tort Statute for lack of subject-matter jurisdiction. ATS MTD, ECF 127. For the reasons below, this Court concludes that Plaintiff does not plead a cognizable tort under the Alien Tort Statute and grants the motion to dismiss that claim.

1. Legal Standard

Federal Rule of Civil Procedure 12(b)(1) provides that a court may dismiss a complaint for lack of subject-matter jurisdiction. A Rule 12(b)(1) jurisdictional challenge may be either "facial" or "factual." *Safe Air for Everyone v. Meyer*, 373 F.3d 1035, 1039 (9th Cir. 2004). In a facial attack, "the challenger asserts that the allegations contained in a complaint are insufficient on their face to invoke federal jurisdiction." *Id.* Facial attacks require the court to assume all allegations in the complaint are true and draw all reasonable inferences in the plaintiff's favor. *Wolfe v. Strankman*, 392 F.3d 358, 362 (9th Cir. 2004) *overruled on other grounds by Munoz v. Superior Ct. of L.A. Cnty.*, 91 F.4th 977 (9th Cir. 2024). A factual attack, by contrast, "disputes the truth of the allegations that, by themselves, would otherwise invoke federal jurisdiction." *Meyer*, 373 F.3d at 1039. In resolving a factual attack on jurisdiction, the court may review evidence beyond the complaint. *Id.*

2. *Sosa* Two-Step Test

The Alien Tort Statute ("ATS") grants federal district courts "original jurisdiction of any civil action by an alien for a tort only, committed in violation of the law of nations or a treaty of the United States." 28 U.S.C. § 1350. The ATS is a purely jurisdictional statute and does not itself identify the torts that may violate the law of nations or a federal treaty. *Sosa v. Alvarez-Machain*, 542 U.S. 692, 712 (2004).

The Supreme Court has identified three inferred private rights of action under the ATS: "violation of safe conducts, infringement of the rights of ambassadors, and piracy." *Sosa*, 542 U.S. at 724. Plaintiff concedes that her claim does not fall within any of these three categories of torts. Opposition to ATS MTD, ECF 132 at 11. Instead, she asks this Court to recognize "persecution" as a cause of action under the ATS. *Id.* This Court declines to do so.

In *Sosa v. Alvarez-Machain*, the Supreme Court held that the ATS "enable[s] federal courts to hear claims in a very limited category defined by the law of nations and recognized at common law." 542 U.S. at 712. This category includes "three historical torts: 'violation of safe conducts, infringement of the rights of ambassadors, and piracy." *Nestlé USA, Inc. v. Doe*, 141 S. Ct. 1931, 1937 (2021) (plurality op.) (quoting *Sosa*, 542 U.S. at 724). In *Sosa*, the Supreme Court recognized that this category may also include other causes of action that "rest on a norm of international character accepted by the civilized world and defined with a specificity comparable to" the three historic causes of action. *Id.* at 725. Warning that courts must exercise "great caution in adapting the law of nations to private rights," the Court intentionally imposed a "high bar" to recognizing new causes of action. *Id.* at 728.

Sosa creates a two-step test for recognizing a new cause of action. First, the court must determine whether the claim violates a "specific, universal, and obligatory" norm of international law. *Sosa*, 542 U.S. at 732. If the answer is yes, the court must then consider whether there is "even one 'sound reason to think that Congress might doubt the efficacy or necessity of the new remedy.'" *Nestlé USA*, 141 S. Ct. at 1937 (cleaned up) (quoting *Jesner v. Arab Bank, PLC*, 138 S. Ct. 1386, 1402 (2018)). This is an "extraordinarily strict" standard that may be satisfied only "in very limited circumstances." *Id.* at 1937–38. If even one reason is identified, "courts must refrain from creating [a] remedy." *Jesner*, 138 S. Ct. at 1402 (2018). The Supreme Court has

never identified any circumstances in which this test has been satisfied, and has suggested that "a proper application of *Sosa* would preclude courts from ever recognizing any new causes of action under the ATS." *Id.* at 1403.

a. Step one

For the purposes of resolving this motion, this Court finds that Plaintiff adequately alleges a violation of a specific, universal, and obligatory norm of international law. To satisfy step one of *Sosa*, a claim must "rest on a norm of international character accepted by the civilized world and defined with a specificity comparable to the features of the 18th-century paradigms" the Supreme Court has recognized. *Sosa*, 542 U.S. at 725.

Plaintiff's FAC alleges Defendants aided and abetted the Emirati government in discriminatorily persecuting and targeting her "because of her public advocacy in opposition to the policing of the ruling regime in Saudi Arabia." ECF 54 ¶ 230. The individual Defendants argue that these allegations are insufficient to satisfy the first step of the *Sosa* test. ATS MTD, ECF 127 at 8–9. They contend that Plaintiff has only alleged that the individual Defendants aided and abetted the UAE's cyber-surveillance program, which does not rise to the level of a crime against humanity. *Id.* at 8. Plaintiff responds that courts have recognized widespread persecution of perceived dissidents as a crime against humanity, and that crimes against humanity are actionable under the ATS. Opposition to ATS MTD, ECF 132 at 11–13.

This Court finds it unnecessary at this stage to resolve whether Plaintiff's alleged tort of persecution, FAC, ECF 54 ¶ 228, is a violation of a universal norm of international law or whether the UAE is engaged in a campaign of persecution against political dissidents, *id.* ¶ 229.[17] More narrowly, Plaintiff alleges that she was arbitrarily detained and tortured, *id.* ¶¶ 20,

[17] This Court notes, however, that most of the cases Plaintiff cites as recognizing persecution as an actionable tort under the ATS were decided before the Supreme Court issued

32–34, and that the individual Defendants' actions aided detention and torture through their surveillance program, *id.* ¶¶ 165, 169, 171, 230. The Ninth Circuit has held that "acts of official torture" and "prolonged arbitrary detention" are universally recognized as violations of established international law, *Siderman de Blake v. Republic of Argentina*, 965 F.2d 699, 716–17 (9th Cir. 1992) (citing Restatement (Third) of Foreign Relations Law § 702 (Am. L. Inst. 1987)), and that aiding-and-abetting liability is available under the ATS, *Doe I v. Cisco Sys., Inc.*, 73 F.4th 700, 717–18 (9th Cir. 2023), *petition for cert. filed*, No. 24-856 (Feb. 11, 2025). For the purposes of resolving this motion and reaching the second step of the *Sosa* test, this Court will assume without deciding that Plaintiff's allegations of torture and arbitrary detention are sufficient to survive step one of the *Sosa* test.

b. Step two

Although Plaintiff has arguably identified violations of specific, universal, and obligatory norms, she has not shown that this Court should infer a cause of action for those violations. Under the second prong of the *Sosa* test, sound reasons exist to think that Congress would doubt the efficacy or necessity of providing an ATS remedy under these circumstances. *See Jesner*, 138 S. Ct. at 1402.[18]

This step requires a court to consider the "practical consequences" of recognizing a new cause of action. *Sosa*, 542 U.S. at 732–33. Among other factors, courts should consider

---

its opinions in *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108 (2013), *Jesner*, 138 S. Ct. 1386, and *Nestlé USA*, 141 S. Ct. 1931, which together sharply narrowed the possible scope of ATS liability.

[18] Because this Court concludes that Plaintiff does not allege a cognizable tort under the ATS, it need not address whether the presumption against extraterritoriality bars Plaintiff's claims. *See Kiobel v. Royal Dutch Petrol. Co.*, 569 U.S. 108, 124–25 (2013); *Doe I v. Cisco Sys., Inc.*, 66 F. Supp. 3d 1239, 1245 (N.D. Cal. 2014), *aff'd in part, rev'd in part* 73 F.4th 700 (9th Cir. 2023), *petition for cert. filed*, No. 24-856 (Feb. 11, 2025).

"legislative guidance," "the possible collateral consequences of making international rules privately actionable," the possible effect of asserting a "limit on the power of foreign governments over their own citizens," and the "risks of adverse foreign policy consequences." *Id.* at 726–28. The court must consider these potential consequences in light of the purpose of the ATS: to provide a forum in which to adjudicate the "narrow set of violations" of international law that, if not addressed, "threaten[] serious consequences in international affairs" for the United States. *Id.* at 715; *see also Jesner*, 138 S. Ct. at 1406 (explaining that the statute exists to ensure a remedy for violations "in circumstances where the absence of such a remedy might provoke foreign nations to hold the United States accountable").

This Court declines to infer a cause of action under the circumstances of this case. The Supreme Court has cautioned that "[t]he political branches, not the Judiciary, have the responsibility and institutional capacity to weigh foreign-policy concerns." *Jesner*, 138 S. Ct. at 1403. Recognizing a cause of action here—effectively finding that the UAE is committing crimes against humanity and allowing all so affected to sue in U.S. courts—could have serious practical ramifications for the U.S.'s relations with the UAE, a key U.S. ally in the Middle East.[19] *See U.S. Relations With United Arab Emirates*, U.S. Dep't of State (Dec. 9, 2020), https://www.state.gov/u-s-relations-with-united-arab-emirates/ [https://perma.cc/KN72-98Q8]. It would also contradict the ATS's purpose of "promot[ing] harmony in international relations by ensuring foreign plaintiffs a remedy for international-law violations in circumstances where the absence of such a remedy might provoke foreign nations to hold the United States accountable."

[19] This Court asked the parties whether it should solicit a statement of interest from the State Department, noting that this is common practice. ECF 133 (citing *Cisco*, 73 F.4th 700 at 749–51 (Christen, J., concurring in part and dissenting in part)). Plaintiff stated that she believed the Court should resolve the motion "based on the current record," ECF 139, while the individual Defendants stated that they would defer to the Court's discretion, ECF 134.

Jesner, 138 S. Ct. at 1403. Plaintiff provides no reason to think the UAE, Saudi Arabia, or any other nation will seek to hold the U.S. accountable if this Court declines to adjudicate Plaintiff's claims.

Plaintiff reads the Ninth Circuit's decision in *Cisco* as holding that "a claim under the ATS against a private contractor" can never "raise foreign policy concerns." Opposition to ATS MTD, ECF 132 at 15. This Court does not read *Cisco* as announcing such a rule. Rather, *Cisco* emphasizes that this remains a "case-specific" determination. 73 F.4th at 719 (quoting *Sosa*, 542 U.S. at 733 n.21). The step-two in this case is whether allowing *this* claim to proceed against *these* private contractors raises any foreign policy concerns that "preclude[] recognition of a cause of action in [this] case." *Id.* Given the foreign relations concerns that would result from allowing Plaintiff to pursue a claim premised on the UAE's alleged crimes against humanity, FAC, ECF 54 ¶ 229, this Court finds that "case-specific foreign policy considerations . . . present a reason to bar this action." *Cisco*, 73 F.4th at 721.

This Court therefore declines to recognize an inferred cause of action under these circumstances and dismisses Plaintiff's ATS claim for lack of subject-matter jurisdiction. Dismissal is without prejudice, *Freeman v. Oakland Unified Sch. Dist.*, 179 F.3d 846, 847 (9th Cir. 1999) (dismissals for lack of jurisdiction should be without prejudice), and without leave to amend because amendment would be futile. *Abagninin v. AMVAC Chem. Corp.*, 545 F.3d 733, 740 (9th Cir. 2008) (affirming district court's dismissal of the plaintiff's ATS claim without leave to amend).

CONCLUSION

For the reasons stated above, Defendants' motion to dismiss for lack of personal jurisdiction, ECF 126, is DENIED; Defendants' motion to dismiss for failure to state a claim, *id.*, is DENIED. The individual Defendants' motion to dismiss for lack of subject-matter jurisdiction

with respect to the ATS claim, ECF 127, is GRANTED. This case will proceed with Plaintiff's CFAA and conspiracy to violate the CFAA claims.

IT IS SO ORDERED.

DATED this 12th day of August, 2025.

/s/ Karin J. Immergut
Karin J. Immergut
United States District Judge